IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	§	Group Art Unit: 2131
	§	
Traversat, et al.	§	Examiner: Chen, Shin Hon
	§	
	§	Atty. Dkt. No.: 5181-64800
	§	P4979
Serial No. 09/653,227	§	
	§	
	§	
Filed: August 31, 2000	§	
	§	
For: Message Authentication Using Message Gates in a Distributed Computing Environment	§	
	§	
	§	
	§	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice of Appeal filed herewith, Appellants present this Appeal Brief. **No fee should be due for this appeal brief since the appeal brief fee was already paid for a previous appeal in this application that did not receive a decision on the merits and from which prosecution was reopened.** ***See*** **MPEP 1207.04.** Appellants respectfully request that the Board of Patent Appeals and Interferences consider this appeal.

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 011070/0082, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

The appeal in Application No. 09/653,215 is related to the present appeal. One of the grounds of rejection in the present appeal is a provisional double patenting rejection in regard to Application No. 09/653,215. Also, both appeals involve at least some of the same prior art references and the same Examiner.

III. STATUS OF CLAIMS

Claims 1-6, 8-31, 33-47 and 49-72 are pending and stand finally rejected. Claims 7, 32 and 48 are cancelled. Claims 14, 22, 37, 46, 54, 60, 68 and 71 would be allowable if rewritten in independent form (and pending resolution of the provisional double patenting rejection). The rejection of claims 1-6, 8-31, 33-47 and 49-72 is being appealed. A copy of claims 1-6, 8-31, 33-47 and 49-72 as currently pending is included in the Claims Appendix herein below.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for communicating in a distributed computing environment including a client accessing an authentication service to obtain an authentication credential to use a service. A client may access or use an authentication service in various ways. A client process may directly communicate with an authentication service to obtain an authentication credential, in some embodiments. In other embodiments, a gate factory on a client may use an authentication service to obtain a authentication credential to be embedded in messages. In yet other embodiments, a gate factory may create or include its own message gate used to communicate with an authentication service to receive an authentication credential. A client may discover an authentication service from a service advertisement, such as may be stored in a network addressable space service. The advertisement may include an address, such as a URI, for accessing the authentication service. A client may present a client identification token or other information as proof of the client's identity to an authentication service. The authentication service may issue to the client an authentication credential that only the authentication service can create. While in some embodiments an authentication credential may be unique to the particular client, in other embodiments, the credential may be a prearranged credential that all clients of a particular service are to use. *See, e.g.*, Figs. 26a (elements 1000-1004), 26b (elements 1002a-1002c), 41 (element 1010), 42b (elements 1032-1036), 42c (elements 1040-1046), and 43 (elements 1050-1056); p. 13, line 31 – p. 14, line 4; p. 33, lines 5-16; p. 35, line 22 – p. 36, line 4; p. 63, lines 3-12; p. 63, line 24 – p. 64, line 4; p. 66, line 22 – p. 67, line 9; p. 69, lines 8 – 21; p. 84, lines 6-21; p. 86, lines 11-28; p. 91, line 25 – p. 92, line 2; p. 94, lines 1- 21; p. 96, line 20 – p. 97, line 26; p. 98, line 4 – p. 99, line 2; and p. 99, line 6 – p. 100, line 27.

The method also includes determining client capabilities for the client. The client capabilities are capabilities of the service that the client is permitted to use. A distributed computing environment may include a mechanism for client to negotiate access rights to use a services capabilities or a subset of a service's full capabilities. The result of such negotiation may be an authentication credential that conveys to the client the right to use

some or all of a service's capabilities. In one embodiment, information received in a request message may be used to determine the capabilities of the client to use a service. In some embodiments an authentication service, such as one used to obtain an authentication credential, may determine the capabilities of the client upon receiving a client's authentication credential from a service desiring to verify the client's authentication. In other embodiments, the service itself may determine the specific capabilities that a client is allowed to use. The method further includes binding the client capabilities to the authentication credential. In one embodiment, the service may bind the client's capabilities to the authentication credential. *See, e.g.*, Figs. 26a (element 1002), 26b (elements 1002b-1002c), 41 (element 1012), 42b (element 1038), 42c (element 1046), and 43 (element 1056); p. 56, lines 4 – 21; p. 63, lines 14 – 21; p. 64, lines 2-11; p. 67, lines 4 – 9; p. 76, lines 1 – 9; p. 85, lines 2 – 11; p. 92, line 20 – p. 93, line 2; and p. 94, lines 4 – 21.

The client sends a message including the authentication credential to the service and the service uses the authentication service to authenticate the authentication credential received in the message. Credentials may be used to verify the identity and/or rights of a client to use a service. In one embodiment, an authentication credential may be presented each time a client uses a service. In some embodiments, a message gate for a client may present the authentication credential. The service receiving the authentication credential may use the authentication credential to ensure that the authentication credential is valid and belongs to the client. By using the authentication service to authenticate the client, the service may establish a binding of the authentication credential to the identity of the client. The sharing a single authentication services by both a client and service, any variety of authentication protocols may be employed, with the details of the particular authentication protocol being separated from both the client and the service. The service responds to the message if the authentication credential in the message is determined to be authentic as from the client. *See, e.g.*, Figs. 41 (elements 1010-1014), 42b (elements 1030-1038), 42c (element 1046), and 43 (element 1056); p. 13, line 28 – p. 14, line 11; p. 32, line 28 – p. 33, line 16; p. 67, lines 4 – 14; p. 84, lines 23- 30; p. 85, lines 2 – 16; p. 87, line 1 – p. 88, line 27; p. 91, line 25 – p. 92, line 2; p.

92, line 20 – p. 93, line 2; p. 93, line 28 – p. 94, line 21; p. 96, line 20 – p. 99, line 2; and p. 105, line 19 – p. 107, line 27.

Independent claim 17 is directed to a method for communication is a distributed computing environment in which a client obtains a service advertisement for a service. An advertisement may provide a mechanism of addressing and accessing services and/or content within the distributed computing environment. Services in a distributed computing environment may publish, such as on a space service, an advertisement for the service. An advertisement may be represented in XML and may include a message schema and an address for accessing the service. Clients may search for or browse published advertisements. Advertisements may be complete advertisements that include a message schema or interface for accessing the service or may be protected advertisements that don't include such a schema or interface. Service advertisement may also include an address for an authentication service that the client may use to obtain an authentication credential and that the service may use to authenticate the client. *See, e.g.*, Figs. 4 (Discovery Service), 8 (element 132), 11b (element 132), 15 (element 114), 16 (element 500), 18 (elements 200a, 206, 208), 22 (elements 320, 328, 330, 332), 24 (elements 1416 and 1418), and 28 (elements 1225 and 1227); p. 27, lines 13 – 22; p. 28, lines 5 – 16; p. 28, line 26 – p. 29, line 7; p. 29, lines 13 – 23; p. 44, lines 16 – 25; p. 45, lines 10-20; p. 55, line 25 – p. 56, line 2; p. 56, lines 10 – 30; p. 57, line 19 – p. 58, line 8; p. 59, line 5 – p. 61, line 19; p. 62, line 10 – 63, line 12; p. 68, lines 7-26; p. 74, line 2 – p. 75, line 11; p. 75, line 24 – p. 76, line 9; p. 79, line 17- p. 80, line 9; p. 84, lines 6 – 21; p. 86, line 11 – 28; and p. 98, line 28 – p. 99, line 21.

The client sends a request message to the authentication service to obtain an authentication credential to use the service. Please refer to the discussion of claim 1 above for more information regarding a client obtaining an authentication credential to use a service.

The client also generates a message gate for accessing the service. Message gates may provide secure message endpoints in a distributed computing environment. A pair

of message gates may provide a mechanism for communicating requests from client to services and responses from services to clients. Two associated message gates may be used to create a secure atomic bi-directional messaging channel for request-response message passage. Messages gates may allow clients and services to exchange messages in a secure and reliable fashion over any suitable message transport (e.g. HTTP). For a client, a message gate may represent the authority to use some or all of a service's capabilities. In one embodiment, message gates may be created that may only send and/or receive a subset of the total message schema for a service. The message gates may perform verification of the messages against the data representation language message schema to ensure that the message is in the allowed subset of messages. Each message may also include a token or credential that includes information that may allow the receiving gate to verify that the message has not been compromised or altered. A distributed computing environment may include several different types of messages gates for communicating between clients and services. Some gates may support flow control while other gates may support remote method invocation. Other gates may support publish and subscribe message passing for events. Message gates may be created from information, such as a message schema, in an advertisement for a service. Message gates may also incorporate an authentication credential obtained from an authentication service. *See, e.g.*, Figs. 10a (elements 130a, 130b, and 120c), 10b (Generated Message and Data-Verify Code 130), 11a (gate 130a), 11b (gates 130a and 130c), 12 (message gates), 20 (elements 300-310), 22 (elements 330 and 332), 34 (gates 1504 and 1506), 35a and 35b (gate 1504), 41 (elements 1010 through 1012), 42a (elements 1020 through 1024), and 42b (elements 1030 through 1038),; p. 35, line 22 – p. 36, line 4; p. 29, line 27 – p. 44, line 14; p. 47, line 11 – 50, line 3; p. 50, line 24 – p. 52, line 3; p. 53, lines 16 – 29; p. 61, line 27 – p. 62, line 8; p. 84, lines 6 – 30; p. 92, line 15 – p. 93, line 26; p. 97, lines 17 – 26; p. 102, lines 5 – 23; and p. 103, lines 5 – 28.

The message gate may embed the authentication credential in every message from the client to the service. Please refer to the discussion of claim 1 above for more information regarding a message gate embedding an authentication credential in every message from a client to a service.

Independent claim 27 recites a client device configured to access an authentication service to obtain an authentication credential to use a service. A client may access or use an authentication service in various ways. A client process may directly communicate with an authentication service to obtain an authentication credential, in some embodiments. In other embodiments, a gate factory on a client may use an authentication service to obtain a authentication credential to be embedded in messages. In yet other embodiments, a gate factory may create or include its own message gate used to communicate with an authentication service to receive an authentication credential. A client may discover an authentication service from a service advertisement, such as may be stored in a network addressable space service. The advertisement may include an address, such as a URI, for accessing the authentication service. A client may present a client identification token or other information as proof of the client's identity to an authentication service. The authentication service may issue to the client an authentication credential that only the authentication service can create. While in some embodiments an authentication credential may be unique to the particular client, in other embodiments, the credential may be a prearranged credential that all clients of a particular service are to use. *See, e.g.*, Figs. 26a (elements 1000-1004), 26b (elements 1002a-1002c), 41 (element 1010), 42b (elements 1032-1036), 42c (elements 1040-1046), and 43 (elements 1050-1056); p. 13, line 31 – p. 14, line 4; p. 33, lines 5-16; p. 35, line 22 – p. 36, line 4; p. 63, lines 3-12; p. 63, line 24 – p. 64, line 4; p. 66, line 22 – p. 67, line 9; p. 69, lines 8 – 21; p. 84, lines 6-21; p. 86, lines 11-28; p. 91, line 25 – p. 92, line 2; p. 94, lines 1- 21; p. 96, line 20 – p. 97, line 26; p. 98, line 4 – p. 99, line 2; and p. 99, line 6 – p. 100, line 27.

The client device of claim 27 is also configured to determine client capabilities for the client device and may also bind the client capabilities to the authentication credential. The client capabilities are capabilities of the service that the client is permitted to use. A distributed computing environment may include a mechanism for client to negotiate access rights to use a services capabilities or a subset of a service's full capabilities. The result of such negotiation may be an authentication credential that

conveys to the client the right to use some or all of a service's capabilities. In one embodiment, information received in a request message may be used to determine the capabilities of the client to use a service. In some embodiments an authentication service, such as one used to obtain an authentication credential, may determine the capabilities of the client upon receiving a client's authentication credential from a service desiring to verify the client's authentication. In other embodiments, the service itself may determine the specific capabilities that a client is allowed to use. The method further includes binding the client capabilities to the authentication credential. In one embodiment, the service may bind the client's capabilities to the authentication credential. *See, e.g.*, Figs. 26a (element 1002), 26b (elements 1002b-1002c), 41 (element 1012), 42b (element 1038), 42c (element 1046), and 43 (element 1056); p. 56, lines 4 – 21; p. 63, lines 14 – 21; p. 64, lines 2-11; p. 67, lines 4 – 9; p. 76, lines 1 – 9; p. 85, lines 2 – 11; p. 92, line 20 – p. 93, line 2; and p. 94, lines 4 – 21.

The client device of claim 27 is further configured to send a message including the authentication credential to the service. The service is configured to use the authentication service to authenticate the authentication credential received in the message. The client device also receives a response to the message from the service if the authentication credential in the message is determine to be authentic as from the client device. The client sends a message including the authentication credential to the service and the service uses the authentication service to authenticate the authentication credential received in the message. Credentials may be used to verify the identity and/or rights of a client to use a service. In one embodiment, an authentication credential may be presented each time a client uses a service. In some embodiments, a message gate for a client may present the authentication credential. The service receiving the authentication credential may use the authentication credential to ensure that the authentication credential is valid and belongs to the client. By using the authentication service to authenticate the client, the service may establish a binding of the authentication credential to the identity of the client. The sharing a single authentication services by both a client and service, any variety of authentication protocols may be employed, with the details of the particular authentication protocol being separated from both the client

and the service. The service responds to the message if the authentication credential in the message is determined to be authentic as from the client. *See, e.g.*, Figs. 41 (elements 1010-1014), 42b (elements 1030-1038), 42c (element 1046), and 43 (element 1056); p. 13, line 28 – p. 14, line 11; p. 32, line 28 – p. 33, line 16; p. 67, lines 4 – 14; p. 84, lines 23- 30; p. 85, lines 2 – 16; p. 87, line 1 – p. 88, line 27; p. 91, line 25 – p. 92, line 2; p. 92, line 20 – p. 93, line 2; p. 93, line 28 – p. 94, line 21; p. 96, line 20 – p. 99, line 2; and p. 105, line 19 – p. 107, line 27.

Independent claim 43 is directed to a service device configured to receive from a client a message including an authentication credential which the obtained by accessing an authentication service. The service device uses the authentication service to authenticate the authentication credential received in the message and determines client capabilities for the client. The service device is additionally configured to bind the client capabilities to the authentication credential and respond to the first message if the authentication credential in the message is determined to be authentic as from the client.

The client sends a message including the authentication credential to the service and the service uses the authentication service to authenticate the authentication credential received in the message. Credentials may be used to verify the identity and/or rights of a client to use a service. In one embodiment, an authentication credential may be presented each time a client uses a service. In some embodiments, a message gate for a client may present the authentication credential. The service receiving the authentication credential may use the authentication credential to ensure that the authentication credential is valid and belongs to the client. By using the authentication service to authenticate the client, the service may establish a binding of the authentication credential to the identity of the client. The sharing a single authentication services by both a client and service, any variety of authentication protocols may be employed, with the details of the particular authentication protocol being separated from both the client and the service. The service responds to the message if the authentication credential in the message is determined to be authentic as from the client. *See, e.g.*, Figs. 41 (elements 1010-1014), 42b (elements 1030-1038), 42c (element 1046), and 43 (element 1056); p.

13, line 28 – p. 14, line 11; p. 32, line 28 – p. 33, line 16; p. 67, lines 4 – 14; p. 84, lines 23- 30; p. 85, lines 2 – 16; p. 87, line 1 – p. 88, line 27; p. 91, line 25 – p. 92, line 2; p. 92, line 20 – p. 93, line 2; p. 93, line 28 – p. 94, line 21; p. 96, line 20 – p. 99, line 2; and p. 105, line 19 – p. 107, line 27.

The service device determines client capabilities for the client. The client capabilities are capabilities of the service that the client is permitted to use. A distributed computing environment may include a mechanism for client to negotiate access rights to use a services capabilities or a subset of a service's full capabilities. The result of such negotiation may be an authentication credential that conveys to the client the right to use some or all of a service's capabilities. In one embodiment, information received in a request message may be used to determine the capabilities of the client to use a service. In some embodiments an authentication service, such as one used to obtain an authentication credential, may determine the capabilities of the client upon receiving a client's authentication credential from a service desiring to verify the client's authentication. In other embodiments, the service itself may determine the specific capabilities that a client is allowed to use. The method further includes binding the client capabilities to the authentication credential. In one embodiment, the service may bind the client's capabilities to the authentication credential. *See, e.g.*, Figs. 26a (element 1002), 26b (elements 1002b-1002c), 41 (element 1012), 42b (element 1038), 42c (element 1046), and 43 (element 1056); p. 56, lines 4 – 21; p. 63, lines 14 – 21; p. 64, lines 2-11; p. 67, lines 4 – 9; p. 76, lines 1 – 9; p. 85, lines 2 – 11; p. 92, line 20 – p. 93, line 2; and p. 94, lines 4 – 21.

Independent claim 51 is directed to a distributed computing system including a client device and a service device. The client device is configured to access an authentication service to obtain an authentication credential to use the service device, determine client capabilities for the client device, bind the client capabilities to the authentication credential, and send a message including the authentication credential to the service device. The service device is configured to use the authentication service to authenticate the authentication credential received in the message and respond to the

message if the authentication credential in the message is determined to be authentic as from the client device.

A client device may access or use an authentication service in various ways. A client process may directly communicate with an authentication service to obtain an authentication credential, in some embodiments. A client device may discover an authentication service from a service advertisement, such as may be stored in a network addressable space service. The advertisement may include an address, such as a URI, for accessing the authentication service. A client device may present a client identification token or other information as proof of the client's identity to an authentication service. The authentication service may issue to the client an authentication credential that only the authentication service can create. While in some embodiments an authentication credential may be unique to the particular client device, in other embodiments, the credential may be a prearranged credential that all client devices of a particular service are to use. *See, e.g.*, Figs. 26a (elements 1000-1004), 26b (elements 1002a-1002c), 41 (element 1010), 42b (elements 1032-1036), 42c (elements 1040-1046), and 43 (elements 1050-1056); p. 13, line 31 – p. 14, line 4; p. 33, lines 5-16; p. 35, line 22 – p. 36, line 4; p. 63, lines 3-12; p. 63, line 24 – p. 64, line 4; p. 66, line 22 – p. 67, line 9; p. 69, lines 8 – 21; p. 84, lines 6-21; p. 86, lines 11-28; p. 91, line 25 – p. 92, line 2; p. 94, lines 1- 21; p. 96, line 20 – p. 97, line 26; p. 98, line 4 – p. 99, line 2; and p. 99, line 6 – p. 100, line 27.

The distributed computing system may also determine client capabilities for the client. The client capabilities are capabilities of the service that the client is permitted to use. A distributed computing environment may include a mechanism for a client device to negotiate access rights to use a services capabilities or a subset of a service's full capabilities. The result of such negotiation may be an authentication credential that conveys to the client the right to use some or all of a service's capabilities. In one embodiment, information received in a request message may be used to determine the capabilities of the client to use a service. In some embodiments an authentication service, such as one used to obtain an authentication credential, may determine the capabilities of the client device, upon receiving a client's authentication credential from a service

desiring to verify the client's authentication. In other embodiments, the service itself may determine the specific capabilities that a client is allowed to use. The distributed computing system may also bind the client capabilities to the authentication credential. In one embodiment, the client device may bind the client's capabilities to the authentication credential. *See, e.g.*, Figs. 26a (element 1002), 26b (elements 1002b-1002c), 41 (element 1012), 42b (element 1038), 42c (element 1046), and 43 (element 1056); p. 56, lines 4 – 21; p. 63, lines 14 – 21; p. 64, lines 2-11; p. 67, lines 4 – 9; p. 76, lines 1 – 9; p. 85, lines 2 – 11; p. 92, line 20 – p. 93, line 2; and p. 94, lines 4 – 21.

The client device sends a message including the authentication credential to the service and the service uses the authentication service to authenticate the authentication credential received in the message. Credentials may be used to verify the identity and/or rights of a client to use a service. In one embodiment, an authentication credential may be presented each time a client device uses a service. The service receiving the authentication credential may use the authentication credential to ensure that the authentication credential is valid and belongs to the client. By using the authentication service to authenticate the client, the service may establish a binding of the authentication credential to the identity of the client. The sharing a single authentication services by both a client and service, any variety of authentication protocols may be employed, with the details of the particular authentication protocol being separated from both the client and the service. The service device responds to the message if the authentication credential in the message is determined to be authentic as from the client device. *See, e.g.*, Figs. 41 (elements 1010-1014), 42b (elements 1030-1038), 42c (element 1046), and 43 (element 1056); p. 13, line 28 – p. 14, line 11; p. 32, line 28 – p. 33, line 16; p. 67, lines 4 – 14; p. 84, lines 23- 30; p. 85, lines 2 – 16; p. 87, line 1 – p. 88, line 27; p. 91, line 25 – p. 92, line 2; p. 92, line 20 – p. 93, line 2; p. 93, line 28 – p. 94, line 21; p. 96, line 20 – p. 99, line 2; and p. 105, line 19 – p. 107, line 27.

Independent claim 58 recites a system including a client device and a service device in which the client device and service device implement the method described above regarding claim 17. An advertisement may provide a mechanism of addressing

and accessing services and/or content within the distributed computing environment. Services in a distributed computing environment may publish, such as on a space service, an advertisement for the service. An advertisement may be represented in XML and may include a message schema and an address for accessing the service. Clients may search for or browse published advertisements. Advertisements may be complete advertisements that include a message schema or interface for accessing the service or may be protected advertisements that don't include such a schema or interface. Service advertisement may also include an address for an authentication service that the client may use to obtain an authentication credential and that the service may use to authenticate the client. *See, e.g.*, Figs. 4 (Discovery Service), 8 (element 132), 11b (element 132), 15 (element 114), 16 (element 500), 18 (elements 200a, 206, 208), 22 (elements 320, 328, 330, 332), 24 (elements 1416 and 1418), and 28 (elements 1225 and 1227); p. 27, lines 13 – 22; p. 28, lines 5 – 16; p. 28, line 26 – p. 29, line 7; p. 29, lines 13 – 23; p. 44, lines 16 – 25; p. 45, lines 10-20; p. 55, line 25 – p. 56, line 2; p. 56, lines 10 – 30; p. 57, line 19 – p. 58, line 8; p. 59, line 5 – p. 61, line 19; p. 62, line 10 – 63, line 12; p. 68, lines 7-26; p. 74, line 2 – p. 75, line 11; p. 75, line 24 – p. 76, line 9; p. 79, line 17- p. 80, line 9; p. 84, lines 6 – 21; p. 86, line 11 – 28; and p. 98, line 28 – p. 99, line 21.

The client sends a request message to the authentication service to obtain an authentication credential to use the service. Please refer to the discussion of claim 1 above for more information regarding a client obtaining an authentication credential to use a service.

The client also generates a message gate for accessing the service. Message gates may provide secure message endpoints in a distributed computing environment. A pair of message gates may provide a mechanism for communicating requests from client to services and responses from services to clients. Two associated message gates may be used to create a secure atomic bi-directional messaging channel for request-response message passage. Messages gates may allow clients and services to exchange messages in a secure and reliable fashion over any suitable message transport (e.g. HTTP). For a client, a message gate may represent the authority to use some or all of a service's

capabilities. In one embodiment, message gates may be created that may only send and/or receive a subset of the total message schema for a service. The message gates may perform verification of the messages against the data representation language message schema to ensure that the message is in the allowed subset of messages. Each message may also include a token or credential that includes information that may allow the receiving gate to verify that the message has not been compromised or altered. A distributed computing environment may include several different types of messages gates for communicating between clients and services. Some gates may support flow control while other gates may support remote method invocation. Other gates may support publish and subscribe message passing for events. Message gates may be created from information, such as a message schema, in an advertisement for a service. Message gates may also incorporate an authentication credential obtained from an authentication service. *See, e.g.*, Figs. 10a (elements 130a, 130b, and 120c), 10b (Generated Message and Data-Verify Code 130), 11a (gate 130a), 11b (gates 130a and 130c), 12 (message gates), 20 (elements 300-310), 22 (elements 330 and 332), 34 (gates 1504 and 1506), 35a and 35b (gate 1504), 41 (elements 1010 through 1012), 42a (elements 1020 through 1024), and 42b (elements 1030 through 1038),; p. 35, line 22 – p. 36, line 4; p. 29, line 27 – p. 44, line 14; p. 47, line 11 – 50, line 3; p. 50, line 24 – p. 52, line 3; p. 53, lines 16 – 29; p. 61, line 27 – p. 62, line 8; p. 84, lines 6 – 30; p. 92, line 15 – p. 93, line 26; p. 97, lines 17 – 26; p. 102, lines 5 – 23; and p. 103, lines 5 – 28.

The message gate may embed the authentication credential in every message from the client to the service. Please refer to the discussion of claim 1 above for more information regarding a message gate embedding an authentication credential in every message from a client to a service.

Independent claim 62 recites a medium including program instructions that are computer-executable to implement the method described above regarding claim 1. A client may access or use an authentication service in various ways. A client process may directly communicate with an authentication service to obtain an authentication credential, in some embodiments. In other embodiments, a gate factory on a client may

use an authentication service to obtain a authentication credential to be embedded in messages. In yet other embodiments, a gate factory may create or include its own message gate used to communicate with an authentication service to receive an authentication credential. A client may discover an authentication service from a service advertisement, such as may be stored in a network addressable space service. The advertisement may include an address, such as a URI, for accessing the authentication service. A client may present a client identification token or other information as proof of the client's identity to an authentication service. The authentication service may issue to the client an authentication credential that only the authentication service can create. While in some embodiments an authentication credential may be unique to the particular client, in other embodiments, the credential may be a prearranged credential that all clients of a particular service are to use. *See, e.g.*, Figs. 26a (elements 1000-1004), 26b (elements 1002a-1002c), 41 (element 1010), 42b (elements 1032-1036), 42c (elements 1040-1046), and 43 (elements 1050-1056); p. 13, line 31 – p. 14, line 4; p. 33, lines 5-16; p. 35, line 22 – p. 36, line 4; p. 63, lines 3-12; p. 63, line 24 – p. 64, line 4; p. 66, line 22 – p. 67, line 9; p. 69, lines 8 – 21; p. 84, lines 6-21; p. 86, lines 11-28; p. 91, line 25 – p. 92, line 2; p. 94, lines 1- 21; p. 96, line 20 – p. 97, line 26; p. 98, line 4 – p. 99, line 2; and p. 99, line 6 – p. 100, line 27.

The method also includes determining client capabilities for the client. The client capabilities are capabilities of the service that the client is permitted to use. A distributed computing environment may include a mechanism for client to negotiate access rights to use a services capabilities or a subset of a service's full capabilities. The result of such negotiation may be an authentication credential that conveys to the client the right to use some or all of a service's capabilities. In one embodiment, information received in a request message may be used to determine the capabilities of the client to use a service. In some embodiments an authentication service, such as one used to obtain an authentication credential, may determine the capabilities of the client upon receiving a client's authentication credential from a service desiring to verify the client's authentication. In other embodiments, the service itself may determine the specific capabilities that a client is allowed to use. The method further includes binding the client

capabilities to the authentication credential. In one embodiment, the service may bind the client's capabilities to the authentication credential. *See, e.g.*, Figs. 26a (element 1002), 26b (elements 1002b-1002c), 41 (element 1012), 42b (element 1038), 42c (element 1046), and 43 (element 1056); p. 56, lines 4 – 21; p. 63, lines 14 – 21; p. 64, lines 2-11; p. 67, lines 4 – 9; p. 76, lines 1 – 9; p. 85, lines 2 – 11; p. 92, line 20 – p. 93, line 2; and p. 94, lines 4 – 21.

The client sends a message including the authentication credential to the service and the service uses the authentication service to authenticate the authentication credential received in the message. Credentials may be used to verify the identity and/or rights of a client to use a service. In one embodiment, an authentication credential may be presented each time a client uses a service. In some embodiments, a message gate for a client may present the authentication credential. The service receiving the authentication credential may use the authentication credential to ensure that the authentication credential is valid and belongs to the client. By using the authentication service to authenticate the client, the service may establish a binding of the authentication credential to the identity of the client. The sharing a single authentication services by both a client and service, any variety of authentication protocols may be employed, with the details of the particular authentication protocol being separated from both the client and the service. The service responds to the message if the authentication credential in the message is determined to be authentic as from the client. *See, e.g.*, Figs. 41 (elements 1010-1014), 42b (elements 1030-1038), 42c (element 1046), and 43 (element 1056); p. 13, line 28 – p. 14, line 11; p. 32, line 28 – p. 33, line 16; p. 67, lines 4 – 14; p. 84, lines 23- 30; p. 85, lines 2 – 16; p. 87, line 1 – p. 88, line 27; p. 91, line 25 – p. 92, line 2; p. 92, line 20 – p. 93, line 2; p. 93, line 28 – p. 94, line 21; p. 96, line 20 – p. 99, line 2; and p. 105, line 19 – p. 107, line 27.

Independent claim 69 recites a medium including program instructions that are computer-executable to implement the method described above regarding claim 17. An advertisement may provide a mechanism of addressing and accessing services and/or content within the distributed computing environment. Services in a distributed

computing environment may publish, such as on a space service, an advertisement for the service. An advertisement may be represented in XML and may include a message schema and an address for accessing the service. Clients may search for or browse published advertisements. Advertisements may be complete advertisements that include a message schema or interface for accessing the service or may be protected advertisements that don't include such a schema or interface. Service advertisement may also include an address for an authentication service that the client may use to obtain an authentication credential and that the service may use to authenticate the client. *See, e.g.*, Figs. 4 (Discovery Service), 8 (element 132), 11b (element 132), 15 (element 114), 16 (element 500), 18 (elements 200a, 206, 208), 22 (elements 320, 328, 330, 332), 24 (elements 1416 and 1418), and 28 (elements 1225 and 1227); p. 27, lines 13 – 22; p. 28, lines 5 – 16; p. 28, line 26 – p. 29, line 7; p. 29, lines 13 – 23; p. 44, lines 16 – 25; p. 45, lines 10-20; p. 55, line 25 – p. 56, line 2; p. 56, lines 10 – 30; p. 57, line 19 – p. 58, line 8; p. 59, line 5 – p. 61, line 19; p. 62, line 10 – 63, line 12; p. 68, lines 7-26; p. 74, line 2 – p. 75, line 11; p. 75, line 24 – p. 76, line 9; p. 79, line 17- p. 80, line 9; p. 84, lines 6 – 21; p. 86, line 11 – 28; and p. 98, line 28 – p. 99, line 21.

The client sends a request message to the authentication service to obtain an authentication credential to use the service. Please refer to the discussion of claim 1 above for more information regarding a client obtaining an authentication credential to use a service.

The client also generates a message gate for accessing the service. Message gates may provide secure message endpoints in a distributed computing environment. A pair of message gates may provide a mechanism for communicating requests from client to services and responses from services to clients. Two associated message gates may be used to create a secure atomic bi-directional messaging channel for request-response message passage. Messages gates may allow clients and services to exchange messages in a secure and reliable fashion over any suitable message transport (e.g. HTTP). For a client, a message gate may represent the authority to use some or all of a service's capabilities. In one embodiment, message gates may be created that may only send

and/or receive a subset of the total message schema for a service. The message gates may perform verification of the messages against the data representation language message schema to ensure that the message is in the allowed subset of messages. Each message may also include a token or credential that includes information that may allow the receiving gate to verify that the message has not been compromised or altered. A distributed computing environment may include several different types of messages gates for communicating between clients and services. Some gates may support flow control while other gates may support remote method invocation. Other gates may support publish and subscribe message passing for events. Message gates may be created from information, such as a message schema, in an advertisement for a service. Message gates may also incorporate an authentication credential obtained from an authentication service. *See, e.g.*, Figs. 10a (elements 130a, 130b, and 120c), 10b (Generated Message and Data-Verify Code 130), 11a (gate 130a), 11b (gates 130a and 130c), 12 (message gates), 20 (elements 300-310), 22 (elements 330 and 332), 34 (gates 1504 and 1506), 35a and 35b (gate 1504), 41 (elements 1010 through 1012), 42a (elements 1020 through 1024), and 42b (elements 1030 through 1038),; p. 35, line 22 – p. 36, line 4; p. 29, line 27 – p. 44, line 14; p. 47, line 11 – 50, line 3; p. 50, line 24 – p. 52, line 3; p. 53, lines 16 – 29; p. 61, line 27 – p. 62, line 8; p. 84, lines 6 – 30; p. 92, line 15 – p. 93, line 26; p. 97, lines 17 – 26; p. 102, lines 5 – 23; and p. 103, lines 5 – 28.

The message gate may embed the authentication credential in every message from the client to the service. Please refer to the discussion of claim 1 above for more information regarding a message gate embedding an authentication credential in every message from a client to a service.

The summary above describes various examples and embodiments of the claimed subject matter; however, the claims are not necessarily limited to any of these examples and embodiments. The claims should be interpreted based on the wording of the respective claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-6, 8-31, 33-47 and 49-72 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-47 of co-pending Application No. 09/653,215.

2. Claims 1, 2, 8-13, 15-17, 20, 21 and 23-26 stand finally rejected under 35 U.S.C. § 102(a) as being anticipated by Adams (U.S. Patent 6,718,470).

3. Claims 3-6, 18 and 19 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of Czerwinski, et al. ("An Architecture for a Secure Service Discovery Service") (hereinafter "Czerwinski").

4. Claims 27-31, 33-36, 38-45, 47, 49-53, 55-59, 61-67, 60, 70 and 72 stand finally rejected under 35 U.S.C. § 102(a) as being anticipated by Adams.

5. Claims 27-31, 33-36, 38-45, 47, 49-53, 55-59, 61-67, 60, 70 and 72 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of Czerwinski.

VII. ARGUMENT

First Ground of Rejection

Claims 1-6, 8-31, 33-47 and 49-72 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-47 of co-pending Application No. 09/653,215. **Appellants note that in the Examiner's Answer dated October 4, 2006, the Examiner withdrew this rejection based on amendment to the co-pending Application No. 09/653,215.** It is not clear why the Examiner has now re-asserted this rejection. The Examiner did not provide any reason for re-asserting this rejection after it was previously withdrawn. Appellants traverse this rejection for at least the following reasons.

The Examiner has not stated a *prima facie* obviousness-type double patenting rejection.

Appellants traverse this rejection on the grounds that the Examiner has not stated a *prima facie* rejection. The only support given by the Examiner for the rejection is that "both applications are claiming [a] method for accessing a service in a distributed computing environment in which a client request[s] capability credentials to access [a] portion of a service through advertisement." However, simply because both applications claim some overlap in subject matter is not a proper reason for holding the claims of the present application obvious from the claims of the listed applications. According to MPEP 804.II.B.1, "the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection." This section of the MPEP also states that the same "factual inquires … that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are employed when making an obviousness-type double patenting analysis." MPEP 804.II.B.1 also states that the Examiner should list the differences between **each** rejected claim and the claims of the other patent/application, and for **each** difference the Examiner should give the reasons why a person of ordinary skill in the art would conclude that the invention

defined in the claim is an obvious variation of the invention defined in a claim of the other patent/application. Simply stating that the claims both recite some overlap in subject matter is not a valid reason why a person of ordinary skill in the art would conclude that the invention defined in each claim is an obvious variation of the invention defined in a claim of the other patent/application. Nor has the Examiner specifically addressed **each difference** of **each claim** of the present application compared to the claims of the other applications. Instead, the Examiner improperly lumped all the claims together and did not address each specific difference. The Examiner clearly has not met the requirements stated in MPEP 804.II.B.1 to establish a *prima facie* obviousness-type double patenting rejection.

Accordingly, Appellants respectfully request removal of the double patenting rejection of claims 1-6, 8-31, 33-47, and 49-72.

Second Ground of Rejection

Claims 1, 2, 8-13, 15-17, 20, 21 and 23-26 stand finally rejected under 35 U.S.C. § 102(a) as being anticipated by Adams (U.S. Patent 6,718,470). Appellants traverse this rejection for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 1, 8, 15 and 16:

1. Adams fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use.

Regarding claim 1, contrary to the Examiner's assertion, Adams fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use. Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege

certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams' centralized privilege data selector. Additionally, **in the Examiner's Answer dated October 4, 2006**, the Examiner argues that Adams' "centralized privilege data selector determines the capabilities of [a] subscriber by using the subscriber's identification to retrieve attribute certificate associated with the subscriber" (Examiner's Answer, page 13, lines 11-13). **However, the Examiner's interpretation of Adams is incorrect. Adams does not describe his privilege data selector as determining client capabilities.** Instead, Adams teaches that the privilege data selector selects among subscriber privilege data "based on the privilege test criteria data." The Examiner's cited passage does not describe *determining a client's capabilities*. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Adams' teaches that privilege data "may be any suitable data required by a relying party to facilitate, for example, acceptance, granting or access decision[s] related to a subscriber unit or user of a subscriber unit" (Adams, column 3, lines 35-38). Adams gives as examples of privilege data, "data representing a user position in a company" and "transaction signing limits" (Adams, column 3, lines 38-41). The type of privilege data used in Adams' system and

selected by the privilege data selector clearly fails to represent client capabilities that are capabilities of a service that the client is permitted to use, as recited in claim 1.

Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as a user's position in a company, to the supplied test criteria data. Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

2. Adams fails to disclose binding the client capabilities to the authentication credential.

Further in regard to claim 1, Adams also fails to disclose binding the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential.

In the Examiner's Answer dated October 4, 2006 the Examiner cites column 6, line 65 to column 7, lines 2 and again asserts that Adams' matching attributes certificates are sent as pre-qualification data. **However, the cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit.** Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Adams' system uses test criteria data and pre-qualification privilege data to avoid having clients sending unnecessary privilege information. When sending pre-qualification privilege data, Adams' system does not bind any client capabilities to an authentication credential.

Furthermore, Adams clearly teaches that the matching attribute certificates are obtained from an attribute certificate repository and returned as pre-qualification privilege data. Adams does not mention anything about binding anything with the attribute certificates, which the Examiner considers the authentication credential of claim 1. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

3. Adams fails to disclose the service using the authentication service to authenticate the authentication credential received in the message from the client.

Additionally in regard to claim 1, Adams fails to disclose the service using the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1.

Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector, which the Examiner equates to the authentication service of claim 1, to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams'

system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

In the Examiner's Answer dated October 4, 2006, the Examiner cites column 6, line 61 to column 7, line 9 and refers to Adams' pre-qualification privilege data being generated by the authentication service/centralized privilege data selector "so that it can be verified by the first service/relying party." The Examiner further asserts, "thus, the first service uses the authentication service to authenticate subscribers based prior to grant[ing] access to subscribers." **However, as noted above, Adams' relying unit receives the pre-qualification privilege data from the centralized privilege data selector and then *compares the test criteria data with the pre-qualification privilege data* as a pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential. Adams clearly teaches that the relying unit performs this comparison on its own. Thus, the relying unit only receives the pre-qualification privilege data from the privilege data selector. It does not use the privilege data selector to perform the pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential.**

4. The Examiner has neglected the standard for anticipation.

Anticipation requires the presence in a single prior art reference disclosure of each and every limitation of the claimed invention, arranged as in the claim. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical invention** must be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, Adams clearly fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use, binding the client capabilities to the authentication credential, and the service using the authentication service to authenticate the authentication credential received in the message from the client. Therefore, Adams

clearly cannot be said to anticipate claim 1.

Thus, for at least the reasons above, the rejection of claim 1 is not supported by the prior art and removal thereof is respectfully requested.

Claim 2:

Regarding claim 2, Adams fails to disclose a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service.

The Examiner cites FIG. 5 and column 6, lines 31-40 of Adams. However, the cited portions make no mention of a client obtaining an address for the authentication service from an advertisement for the service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. Nowhere does Adams describe a client obtaining an address for the authentication service from an advertisement for the service.

In the Examiner's Answer dated October 4, 2006, the Examiner also cites column 5, lines 14 – 17 and column 6, lines 49-51. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's**

conclusion. Instead, the Examiner is merely speculating regarding the workings of Adams' system.

Firstly, at the Examiner's cited passage, Adams states that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. Secondly, the cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service advertisement, Adams cannot be said to anticipate a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

Thus, for at least the reasons above, the rejection of claim 2 is not supported by the cited art and removal thereof is respectfully requested.

Claim 9:

Regarding claim 9, Adams fails to disclose that determining client capabilities includes the client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. The Examiner cites column 6, lines 31-67. The cited passage describes use of a centralized privilege data selector in Adams' system. Adams teaches that a relying unit communicates privilege test criteria data to the centralized privilege data selector and that a subscriber unit sends privilege verification request data including subscriber identification data and selected relying party identification data to the centralized privilege data selector. The centralized privilege data selector uses the subscriber identification data to obtain the appropriate attribute certificates from an attributes certificate repository and uses the relying party identification data to obtain the correct privilege test data for the identified relying party unit. However, the cited passage does not mention a client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. Adams' centralized privilege data selector sends attribute certificates that match the privilege test data to the subscriber unit.

In the Examiner's Answer dated October 4, 2006, the Examiner argues that Adams' "pre-qualification privilege data includes the capabilities of the service that the subscriber is permitted to access." **However, the Examiner's interpretation of Adams is incorrect.** Nowhere does Adams mention a client obtaining a capability token indicating which capabilities of the service the client is permitted to access. Adams attribute certificates include such certificates as Kerberos tickets, DCE PAC, etc. that do not indicate which capabilities of a service the client is permitted to access. Additionally, Adams states that the privilege data "may be data representing a user position in a company (e.g., an employee or independent contractor), transaction signing limits, or other suitable data" (parenthesis in original, Adams, column 3, lines 38-41). Thus, Adams' privilege data, including pre-qualification privilege data, does not refer to

capabilities of a particular service that a subscriber is permitted to access, as asserted by the Examiner.

Thus, for at least the reasons above, the rejection of claim 9 is not supported by the cited art and removal thereof is respectfully requested.

Claim 10:

Regarding claim 10, Adams fails to disclose an authentication service and an access policy service that are combined as a single service and where the capability token is included within the authentication credential. The Examiner cites column 6, lines 31-67. However, the cited passage fails to mention anything about an authentication service and an access policy service combined as a single service. The cited passage also fails to mention a capability token included within an authentication credential. The cited passage describes centralized privilege data selector that receives information from both a relying unit and subscriber unit and that returns matching attribute certificates to the subscriber unit. Nowhere does Adams describe either a combined authentication service and access policy service or a capability token included within an authentication credential.

Thus, for at least the reasons above, the rejection of claim 10 is not supported by the cited art and removal thereof is respectfully requested.

Claim 11:

Regarding claim 11, Adams fails to disclose where determining client capabilities is performed by the service. The Examiner cites column 6, lines 17-20 and refers to the sending of privilege test criteria data to a subscriber unit by a relying unit. However, the sending of privilege test criteria data is not the same as determining client capabilities. Instead, Adams describes that the privilege test criteria indicates the specific privilege information necessary for the relying part to grant privilege to a subscriber unit

(Adams, column 3, lines 47-51). For example, Adams describes privilege test criteria data indicating data representing a required membership or indicating the public key certificates that the relying unit would consider for authentication purposes (Adams, column 5, lines 37-40 and column 7, lines 47-55). Thus, the relying unit, which the Examiner equates to the service of Applicants' claims, does not perform the determining of client capabilities, but instead provides privilege test criteria data indicating what types of privilege data it would recognize or consider before granting the subscriber unit privilege.

Thus, for at least the reasons above, the rejection of claim 11 is not supported by the cited art and removal thereof is respectfully requested.

Claim 12:

Regarding claim 12, Adams fails to disclose the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential in each message to the first service. The Examiner cites column 6, line 67 – column 7, line 8 of Adams. However, the cited passage makes no mention whatsoever regarding a client generating a message gate or about the message gate including an authentication credential in each message to the service. The cited passage merely states that Adams' subscriber unit sends pre-qualification attributes or privilege data to the relying unit "through a suitable communication link". However, merely stating that the pre-qualification attributes are sent through a suitable communication link does not disclose the specific limitations of generating a message gate or about a message gate including an authentication credential in each message to the service. Nowhere does Adams mention anything regarding either message gates or about including an authentication credential in each message to the first service.

In the Examiner's Answer dated October 4, 2006, the Examiner also cites column 4, lines 10-11 and column 6, line 67 – column 7, line 2. At the first cited passage

(column 4, lines 10-11) Adams states that his FIG. 1 illustrates "an example of a system for granting security privilege 100 that may be applied to a communication system employing cryptography based security." The second cited passage (column 6, line 67 – column 7, line 2) Adams states that the subscriber unit transmits the pre-qualified attributes or privilege data to the relying party unit through a suitable communication link. The Examiner argues, "[s]ince the communication is encrypted and the pre-qualification privilege data [is] transmitted to the relying party when requesting a service, thus a message gate is generated and the authentication credential [is] included in each message to the first serviced." **However, the fact that the subscriber unit sends the pre-qualification privilege data to the relying unit does not imply that the pre-qualification privilege data, which the Examiner equates with the authentication credential of Applicants' claim, is embedded *with every message* from the subscriber unit to the relying unit.** Adams' system involves using privilege data as part of granting the subscriber unit access to some other application on the relying party. For example, Adams states that after a subscriber unit is granted privilege, "[t]he subscriber unit may then access the relying party". Thus, Adams' subscriber unit clearly sends other messages to the relying party. However, Adams does not that the pre-qualification privilege data is embedded *in every message* sent from the subscriber unit to the relying unit.

Thus, for at least the reasons above, the rejection of claim 12 is not supported by the cited art and removal thereof is respectfully requested.

Claim 13:

Regarding claim 13, Adams fails to disclose the client obtaining a service advertisement for the first service before accessing the first service, where the service advertisement includes an address for the authentication service and an address for the first service. The Examiner cites column 6, lines 31-48. However, this passage does not disclose a client obtaining a service advertisement. Instead, as described above regarding claims 2 and 9, this passage describes a centralized privilege

data selector that receives information from a subscriber unit and a relying unit. However, the subscriber unit, which the Examiner equates to the client of Applicants' claim, does not obtain any service advertisement. Adams fails to mention anything about a service advertisement that includes an address for the authentication service and an address for the first service.

In the Examiner's Answer dated October 4, 2006, the Examiner also cites column 5, lines 14 – 17 and column 6, lines 49-51. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's conclusion.** Instead, the Examiner is merely speculating regarding the workings of Adams' system.

As described above regarding claim 2, Adams states that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. Secondly, the cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it

would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service advertisement, Adams cannot be said to anticipate a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

Adams clearly fails to disclose the client obtaining a service advertisement for the first service before accessing the first service, where the service advertisement includes an address for the authentication service and an address for the first service. Thus, for at least the reasons above, the rejection of claim 13 is not supported by the cited art and removal thereof is respectfully requested.

Claims 17, 25 and 26:

Regarding claim 17, Adams fails to disclose a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. The Examiner cites column 6, lines 31-67. However, the cited passage makes no mention of a client obtaining a service advertisement that includes an address for an authentication service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. No mention is made in the cited passage regarding a client obtaining a service advertisement for a service, where the service advertisement includes an address for an

authentication service. According to the Examiner's interpretation, Adams' subscriber would have to obtain a service advertisement for the relying party unit and the service advertisement would have to include an address for the centralized privilege data selector. However, Adams system does not include any service advertisement for a relying party unit that includes an address for the centralized privilege data selector. The Examiner has clearly misinterpreted the teachings of Adams.

In the Examiner's Answer dated October 4, 2006, the Examiner also cites column 5, lines 14 – 17 referring to the fact that a user in Adams' system may use a website of the relying party. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's conclusion.** Instead, the Examiner is merely speculating regarding the workings of Adams' system.

As described above regarding claim 2, Adams states, at the Examiner's cited passage, that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. The cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an

address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service advertisement, Adams cannot be said to anticipate a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

Adams further fails to disclose the client generating a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client to the service. The Examiner cites column 6, lines 65-67 where Adams states that any matching attribute certificates are sent as pre-qualification privilege data back to the subscriber unit and that the subscriber unit then transmits the pre-qualification privilege data to the relying unit through a suitable communication link. The cited passage does not mention anything about the subscriber unit, which the Examiner considered a client, generating a message gate that embeds the authentication credential in every message from the client to the service. The mere mention of "a suitable communication link" does not disclose the specific limitation of generating a message gate that embeds an authentication credential in every message. Adams does not describe, either at the cited passage or elsewhere, anything about message gates or embedding an authentication credential in every message from a client to a service. The Examiner is merely relying upon speculation, which is clearly improper.

In the Examiner's Answer dated October 4, 2006, the Examiner also cites column 4, lines 10-11 and column 6, line 67 – column 7, line 2. At the first cited passage (column 4, lines 10-11) Adams states that his FIG. 1 illustrates "an example of a system for granting security privilege 100 that may be applied to a communication system

employing cryptography based security." The second cited passage (column 6, line 67 – column 7, line 2) Adams states that the subscriber unit transmits the pre-qualified attributes or privilege data to the relying party unit through a suitable communication link. The Examiner argues, "[s]ince the communication is encrypted and the pre-qualification privilege data [is] transmitted to the relying party when requesting a service, thus a message gate is generated and the authentication credential [is] included in each message to the first serviced." **However, the fact that the subscriber unit sends the pre-qualification privilege data to the relying unit does not imply that the pre-qualification privilege data, which the Examiner equates with the authentication credential of Applicants' claim, is embedded *with every message* from the subscriber unit to the relying unit.** Adams' system involves using privilege data as part of granting the subscriber unit access to some other application on the relying party. For example, Adams states that after a subscriber unit is granted privilege, "[t]he subscriber unit may then access the relying party". Thus, Adams' subscriber unit clearly sends other messages to the relying party. However, Adams does not that the pre-qualification privilege data is embedded *in every message* sent from the subscriber unit to the relying unit.

Thus, for at least the reasons above, the rejection of claim 17 is not supported by the cited art and removal thereof is respectfully requested.

Claim 20:

Regarding claim 20, Adams does not disclose the first service using the authentication service to determine if the authentication credential received in a first message from the client is authentic. The Examiner cites column 6, lines 17-20 and refers to Adams' relying unit sending test criteria data to the subscriber unit. However, the cited passage is not described the relying unit, which the Examiner equates to the first service of Applicants' claim, using the centralized privilege data selector, which the Examiner equates to the authentication service of Applicants' claim, to determine if an authentication credential received in a message from a client is authentic.

Instead, the cited passage describes a subscriber unit requesting privilege test criteria data, which Adams describes as indicating the privilege data the relying unit would accept or consider, from the relying unit. In fact, in the very next sentence Adams states, "[i]t should be recognized that the subscriber unit 400 need not be authenticated by the relying party unit." Thus, the cited passage clearly fails to disclose the first service using the authentication service to determine if the authentication credential received in a message from the client is authentic.

In the Examiner's Answer dated October 4, 2006, the Examiner cites column 6, line 61 to column 7, line 9 and refers to Adams' pre-qualification privilege data being generated by the authentication service/centralized privilege data selector "so that it can be verified by the first service/relying party." The Examiner further asserts, "thus, the first service uses the authentication service to authenticate subscribers based [ ] to grant[ing] access to subscribers." **However, as noted above, Adams' relying unit receives the pre-qualification privilege data from the centralized privilege data selector and then *compares the test criteria data with the pre-qualification privilege data* as a pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential. However, Adams clearly teaches that the relying unit performs this comparison on its own. Thus, the relying unit only receives the pre-qualification privilege data from the privilege data selector. It does not use the privilege data selector to perform the pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential.**

Moreover, even when Adams' relying unit determines whether the pre-qualification privilege data it receives from a subscriber unit is correct, it does not involve the relying unit using the centralized privilege data selector, which the Examiner equates to an authentication service. Instead, the relying unit compares the pre-qualification privilege data it receives to its own privilege test criteria data to ensure it matches (Adams, column 6, lines 25-30 and column 7, lines 5-9).

Thus, for at least the reasons above, the rejection of claim 20 is not supported by the cited art and removal thereof is respectfully requested.

Claim 21:

Regarding claim 21, Adams fails to disclose where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. The Examiner cites column 7, lines 3-8. However, the cited passage fails to describe the relying unit responding to a request message from the client *only if the request message is for an authorized capability for the client.* Adams teaches that the relying unit sends a confirmation message "indicating whether the relying party has granted privilege to the subscriber unit" (Adams, column 6, lines 25-30). Thus, the relying unit responds to the message (with a confirmation message) whether or not the request message is for an authorized capability for the client. The relying unit may not grant the subscriber unit privilege, but Adams' clearly teaches that it responds with a confirmation message.

In the Examiner's Answer dated October 4, 2006, the Examiner argues that the "definition of 'responds' interpreted by the examiner is when access is granted". However, such an interpretation is not supported by Adams. As noted above, Adams clearly describes the relying unit *responding* to a request from the subscriber unit by sending a confirmation message indicating whether the relying has granted privilege to the subscriber unit. Thus, Adams clearly teaches that the relying unit, which the Examiner equates to the service of Applicants' claims, responds to requests regardless of whether the request is for an authorized capability for the client.

Thus, for at least the reasons above, the rejection of claim 21 is not supported by the cited art and removal thereof is respectfully requested.

Claim 23:

Regarding claim 23, the rejection of claim 23 is improper because claim 23 is rejected under 35 U.S.C. § 102(a) as being anticipated by Adams but the Examiner admits in the rejection that "Adams does not explicitly disclose said first service noting whether or not said authentication credential is authentic so that said first service does not need to repeat said using said authentication service to determine if said authentication credential received in a first message from a client is authentic." Thus, the Examiner admits that Adams fails to anticipate claim 23. The Examiner further argues that since Single-Sign-On is well known in the art, "it would have been obvious" to allow the system to note whether the authentication credential is authentic to avoid repeating the authentication process. Firstly, the Examiner is making an obviousness-type rejection, which is improper rejection under 35 U.S.C. § 102(a). Secondly, the Examiner merely states a broad conclusion that Single-Sign-On is well known, without providing any supporting evidence to show that Single-Sign-On discloses the limitations of claim 23 nor that Single-Sign-On was well known at the time Applicants' invention was made.

In the Examiner's Answer dated October 4, 2006, the Examiner states, "Adams might not have explicitly disclosed the limitation of claim 23, but Adams inherently discloses that the Single-Sign-On can be applied for services controlled by the same relying party." However, Adams makes no mention of Single-Sign-On. The Examiner does not cite any portion of Adams where Single-Sign-On is inherently disclosed. Instead, the Examiner merely states that Single-Sign-On is well-known and that Adams inherently discloses that Single-Sign-On can be applied for services controlled by the same relying party. The Examiner is incorrect and his assertions are not supported by any evidence of record.

Furthermore, as the Examiner is surely aware, "[t]o serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence" and that "[s]uch evidence **must make**

clear that the missing descriptive matter is necessarily present in the thing described n the reference, and that it would be so recognized by persons of ordinary skill" (emphasis added, M.P.E.P. § 2131.01 III). The Examiner has not provided any such extrinsic evidence. Instead, the Examiner has merely stated that Adams inherently discloses Single-Sign-On. Thus, without some extrinsic evidence showing that Single-Sign-On is ***necessarily*** present in Adams' system, Adams clearly fails to anticipate claim 23.

Thus, the rejection of claim 23 is clearly improper and not supported by the cited art. Removal of the rejection of claim 23 is respectfully requested.

Claim 24:

Regarding claim 24, Adams fails to disclose a service advertisement for the first service that includes an address for accessing the first service. The Examiner cites column 6, lines 31-41. However, this passage makes no mention of any service advertisement for the first service that includes an address for accessing the first service. As described previously, the cited passage describes Adams' centralized privilege data selector. Nowhere does Adams describe any sort of service advertisement including an address for the service. The Examiner fails to cite and portion of Adams or provide any interpretation of Adams' teachings that disclose a service advertisement for the first service that includes an address for accessing the first service.

In the Examiner's Answer dated October 4, 2006, the Examiner again refers to column 5, lines 14 – 17 and column 6, lines 49-51 of Adams. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." **However, claim 24 recites that the service advertisement includes an address *for accessing the first service*. Thus, the Examiner's assertion regarding how the subscriber must be informed of the authentication service's address is irrelevant.**

Thus, for at least the reasons above, the rejection of claim 24 is not supported by the cited art and removal thereof is respectfully requested.

Third Ground of Rejection

Claims 3-6, 18 and 19 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of Czerwinski, et al. ("An Architecture for a Secure Service Discovery Service") (hereinafter "Czerwinski"). Appellants traverse this rejection for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claim 3:

Regarding claim 3, Adams in view of Czerwinski fails to teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach or suggest an advertisement for the first service that includes a data representation language schema defining a message interface for accessing the first service and relies upon Czerwinski. However, Czerwinski does not teach that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. In contrast, Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.

Furthermore, no combination of Adams and Czerwinski teaches or suggests that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Czerwinski discloses that the XML format service description and client queries are used for communication between client and service (Czerwinski: 2.3 and 3.1). Therefore, Czerwinski suggests that XML format can be used for service description and client queries to establish interface between client and service." Applicants note that the Examiner's assertion adds nothing substantial to the Examiner's prior arguments. However, Czerwinski does disclose the use of XML. Czerwinski further discloses that XML may be used for "client queries". **However, as noted above, neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.** Furthermore, a client query using an XML template as the content of a query is very different from a data representation language schema defining a message interface for accessing a service. The XML template in a client query in Czerwinski does not define a message interface for accessing a service. Instead, client queries include desired services and are matched against service descriptions to find services providing those desired services (Czerwinski, section 2.3, paragraph 3 and section 3.1, paragraph 5). Further, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, and not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, Czerwinski clearly fails to teach wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Thus, a client query in Czerwinski is not a data representation schema, and does not define a message interface for accessing a service. As noted above, there is no way in Czerwinski for a client to define such a message interface in a query template when the client has not even located a service (that is purpose of submitting the query template) and it would be

impossible in Czerwinski for the client to define a message interface for a service that has not even been located and/or selected.

Furthermore, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, the clients do not use messages defined in data representation language schemas in Czerwinski's system and certainly do not use messages defined in data representation language schema for submitting queries to SDS servers.

Furthermore, the Examiner's stated motivation to combine the references, "because XML is well known in the art to provide greater flexibility as communication interfaces", is merely conclusory. Neither Adams nor Czerwinski disclose any motivation to combine the two references.

Obviousness cannot be established by combining or modifying the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion or incentive to do so. *In re Bond,* 910 F. 2d 81, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). In addition, the showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular .... Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'." *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). The art must fairly teach or suggest to one to make the specific combination as claimed. That one achieves an improved result by making such a combination is no more than hindsight without an initial suggestion to make the combination. The Examiner has failed to provide a proper *prima facie* case of obviousness.

Furthermore, even if Adams and Czerwinski were combined, the results would not be anything like what is disclosed in claim 3 of the instant application. Combining Adams' "system and method for granting security privilege in a

communication system" with Czerwinski's "architecture for a secure service discovery service", if possible, **would not produce what is recited in claim 3 of the instant application**. The results of such a combination, if possible, would simply be an embodiment of Adams' "system and method for granting security privilege in a communication system" that uses XML for some purpose, which does not anticipate what is recited in claims 1 and 2 from which claim 3 depends.

Thus, for at least the reasons above, the rejection of claim 3 is not supported by the cited art and removal thereof is respectfully requested.

Claim 4:

Regarding claim 4, Adams in view of Czerwinski fails to teach or suggest that the first message, sent from the client to the service and including the authentication credential, corresponds to a message defined in the data representation language schema. The Examiner admits that Adams fails to teach the limitations of claim 4 and relies upon Czerwinski, citing Czerwinski's teachings regarding XML queries. The Examiner cites a portion of Czerwinski (section 3.1) that describes how a client submits a query in the form of an XML template. However, a client query using an XML template as the content of a query is very different from a data representation language schema defining a message interface for accessing a service. The XML template in a client query in Czerwinski does not define a message interface for accessing a service. Instead, client queries include desired services and are matched against service descriptions to find services providing those desired services (Czerwinski, section 2.3, paragraph 3 and section 3.1, paragraph 5). Further, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, and not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, Czerwinski clearly fails to teach wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Thus, a client query in Czerwinski is not a data representation

schema, and does not define a message interface for accessing a service. As noted above, there is no way in Czerwinski for a client to define such a message interface in a query template when the client has not even located a service (that is purpose of submitting the query template) and it would be impossible in Czerwinski for the client to define a message interface for a service that has not even been located and/or selected.

Furthermore, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, the clients do not use messages defined in data representation language schemas in Czerwinski's system and certainly do not use messages defined in data representation language schema for submitting queries to SDS servers.

Thus, the combination of Adams and Czerwinski clearly fails to teach or suggest that the first message, sent from the client to the service and including the authentication credential, corresponds to a message defined in the data representation language schema.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Czerwinski discloses that the XML format service description and client queries are used for communication between client and service (Czerwinski: 2.3 and 3.1). Therefore, Czerwinski suggests that XML format can be used for service description and client queries to establish interface between client and service." The Examiner has added no new arguments beyond the Examiner's previous arguments and those responded to above in reference to claim 3, from which claim 4 depends.

Thus, for at least the reasons above, the rejection of claim 4 is not supported by the cited art and removal thereof is respectfully requested.

Claims 5 and 6:

Regarding claim 5, Adams in view of Czerwinski fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages. The Examiner cites column 6, lines 31 – 67 of Adams. However, Adams does not mention anything regarding including an authentication credential with each additional message sent by the client to the service. Adams only states that the subscriber unit transmits the pre-qualification attributes or privilege data to the relying unit "through a suitable communication link" (Adams, column 6, line 67 – column 7, line 2). Adams fails to mention anything regarding the sending of additional messages or about an authentication credential included in each of the additional messages.

Czerwinski also fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages. Czerwinski teaches that authentication in ARMI "consists of a short handshake that establishes a symmetric [encryption] key used for the rest of the session" and that "ARMI uses certificates to authenticate each of the endpoints" (Czerwinski, page 28, section 3.5.3). Thus, Czerwinski teaches performing a handshake once at the beginning of a session in which certificates are used to authenticate each endpoint and the symmetric encryption key is used for the remainder of the session. Czerwinski does not mention including an authentication credential with each additional message. Even if combined, Adams and Czerwinski fail to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages.

Furthermore, since any additional messages (after the initial handshake) are encrypted and decrypted using the symmetric encryption key, there is not need to include any authentication credential with each message. Hence, **Czerwinski teaches away** from an authentication credential included with each one of the additional messages.

Adams in view of Czerwinski also fails to teach or suggest wherein each one of the additional messages is defined by the data representation language schema. The Examiner cites Czerwinski's teachings regarding XML queries. However, as noted above, regarding the rejection of claims 3 and 4, Czerwinski fails to teach sending message that are defined by a data representation language schema. Thus, Czerwinski clearly fails to teach sending additional message, where each additional message is defined by the data representation language schema. Adams fails, as admitted by the Examiner in the rejection of claim 4, to teach or suggest sending messages defined by a data representation language schema and thus, Adams fails to overcome the deficiencies of Czerwinski regarding sending additional messages where each additional message is defined by the data representation language schema.

Therefore the combination of Adams and Czerwinski clearly fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages wherein each one of the additional messages is defined by the data representation language schema.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses that the relying party checks the pre-qualification privilege data prior to granting privilege to the subscriber (Adams: column 7 lines 5-9). The relying party checks the pre-qualification privilege data every time the subscriber requests access, thus the authentication credential is included with each one of the additional messages". Applicants can find nothing in the cited selection or elsewhere in the Adams reference that teaches or suggests that "the relying party checks the pre-qualification privilege data every time the subscriber requests access", nor can the Applicants find anything in the cited selection or elsewhere in the Adams reference that would lead to the Examiner's conclusion that "thus the authentication credential is included with each one of the additional messages." Again, Adams does not mention anything regarding including an authentication credential with each additional message sent by the client to the service,

and moreover Adams fails to mention anything regarding the sending of additional messages or about an authentication credential included in each of the additional messages.

In the Examiner's Answer dated October 4, 2006, the Examiner further asserts "Applicants further argue that Czerwinski does not disclose the limitation. However, Czerwinski is not relied upon to disclose authentication credential is included with each one of the additional messages." Applicants recognize that the Examiner relies upon Adams to disclose this limitation. **However, Applicants are arguing that the cited references, alone or in combination, do not teach or suggest the limitations of claim 5.**

In the Examiner's Answer dated October 4, 2006, the Examiner further asserts "Applicants argue Czerwinski does not disclose additional messages are defined in the data representation language schema. However, Czerwinski discloses that the XML format service description and client queries are used for communication between client and service (Czerwinski: 2.3 and 3.1). Therefore, Czerwinski suggests that XML format can be used for service description and client queries to establish interface between client and service." Applicants responded to this assertion above in reference to claim 3.

Thus, for at least the reasons above, the rejection of claim 5 is not supported by the cited art and removal thereof is respectfully requested.

Claims 18 and 19:

Regarding claim 18, Adams in view of Czerwinski does not teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach the limitations of claim 18 and relies upon Czerwinski, citing section 2.3 and referring to Czerwinski's XML Service Description. However, the cited section does not describe a service advertisement that includes a data representation

language schema defining a message interface for accessing the service. Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service. For a more detailed discussion regarding Czerwinski's failure to teach *including, in a service advertisement, a data representation language schema defining a message interface for accessing a service*, please see the discussion of claim 3 above.

Additionally, Adams in view of Czerwinski does not teach or suggest the message gate verifies that each message sent from the client to the first service complies with the data representation language schema. The Examiner again cites sections 3.1 of Czerwinski and refers to a client (in Czerwinski) using Authenticated RMI. However, the cited section does not mention any sort of message gate verifying that messages sent from a client to a service comply with a data representation language schema.

As neither Adams nor Czerwinski teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service and that the message gate verifies that each message sent from the client to the first service complies with the data representation language schema, Adams and Czerwinski, whether considered singly or in combination, fail to teach or suggest the limitations of claim 18.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses the subscriber access the relying party service through website (Adams: column 5 lines 13-18). Adams does not disclose the first service includes a data representation language schema defining a message interface for accessing the first

service. However, Examiner relies on Czerwinski to disclose service using XML format to describe service descriptions and client queries (Czerwinski: 2.3). Therefore, Czerwinski suggests that XML format can be used for service description and client queries to establish interface between client and service." **However, as noted above, neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.** Furthermore, a client query using an XML template as the content of a query is very different from a data representation language schema defining a message interface for accessing a service. The XML template in a client query in Czerwinski does not define a message interface for accessing a service. Instead, client queries include desired services and are matched against service descriptions to find services providing those desired services (Czerwinski, section 2.3, paragraph 3 and section 3.1, paragraph 5). Further, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, and not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, Czerwinski clearly fails to teach wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Thus, a client query in Czerwinski is not a data representation schema, and does not define a message interface for accessing a service. As noted above, there is no way in Czerwinski for a client to define such a message interface in a query template when the client has not even located a service (that is purpose of submitting the query template) and it would be impossible in Czerwinski for the client to define a message interface for a service that has not even been located and/or selected.

Furthermore, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, the clients do not use messages defined in data representation language schemas in Czerwinski's

system and certainly do not use messages defined in data representation language schema for submitting queries to SDS servers.

In the Examiner's Answer dated October 4, 2006, the Examiner further asserts "Czerwinski discloses the message gate verifies that the messages are in proper format prior to processing requests (Czerwinski: 2.3: use XML format for client queries; page 27 left column 5th paragraph: the query is in the form of XML). The queries need to comply with the format used by the service so that the service can process query submitted by client." Czerwinski does not disclose a message gate, wherein the message gate verifies that each message sent from the client to the first service complies with the data representation language schema. The Examiner cites sections 3.1, page 27 left column 5th paragraph, of Czerwinski. However, this paragraph makes no reference whatsoever to any sort of message gate verifying that messages sent from a client to a service comply with a data representation language schema, nor does any other section of Czerwinski. Furthermore, as described previously, Czerwinski teaches the use of Authenticated RMI that, as noted above, does not use data representation language schemas and thus does not include any message gate verifying that messages comply with a data representation language schema (See, page 28, section 3.5.3).

Thus, for at least the reasons above, the rejection of claim 18 is not supported by the cited art and removal thereof is respectfully requested.

Furthermore, claim 18 recites limitations similar to claim 14, which the Examiner indicates would be allowable if rewritten in independent form.

Fourth Ground of Rejection

Claims 27-31, 33-36, 38-45, 47, 49-53, 55-59, 61-67, 69, 70 and 72 stand finally rejected under 35 U.S.C. § 102(a) as being anticipated by Adams. Appellants traverse this rejection for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 27, 33, 38, 39, 41 and 42:

Regarding claim 27, contrary to the Examiner's assertion, Adams fails to disclose a client device configured to determine client capabilities for the client device, where the client capabilities are capabilities of the first service that the client device is permitted to use. As described above regarding claim 1, Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams' centralized privilege data selector. However, the cited passage does not describe determining a client's capabilities. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as may be stored in a certificate repository, to the supplied test criteria data. Adams does not describe his privilege data selector as determining client capabilities. Instead, Adams teaches that the privilege data selector selects among subscriber privilege

data "based on the privilege test criteria data." Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

Adams also fails to disclose the client device configured to bind the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential. The cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit. Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

Additionally, Adams fails to disclose the service configured to use the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege

verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses determining client capabilities for a client (Adams: column 6 lines 52-55 and 58-60: the centralized privilege data selector obtains the attributes certificate of subscribers from attributes certificate repository according to subscriber's identification data). The centralized privilege selector determines the capabilities of subscriber by using the subscriber's identification data to retrieve attribute certificate associated with the subscriber." **Again, Adams in the cited selection fails to mention anything about determining the client's capabilities**, where the client capabilities are capabilities of the first service that the client is permitted to use. The cited passage does not describe determining a client's capabilities. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers.

In the Examiner's Answer dated October 4, 2006, the Examiner further asserts "Adams also discloses binding the client capabilities to the authentication credential (Adams: col. 6 line 65 - column 7 line 2: the matching attributes certificates are sent as pre-qualification data). The capabilities/attribute certificates of client are sent to clients in form of pre-qualification privilege data/authentication credential." The matching attribute certificates referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. **Nowhere does Adams mention binding determined client capabilities to an authentication credential**.

In the Examiner's Answer dated October 4, 2006, the Examiner further asserts "Adams discloses using the authentication service to authenticate the authentication credential (Adams: column 6 line 61 - column 7 line 9: the pre-qualification privilege data). The pre-qualification privilege data is generated by the authentication service/centralized privilege data selector so that it can be verified by the first service/relying party, thus the first service uses the authentication service to authenticate subscribers based prior to grant access to subscribers. Therefore, Adams discloses all the limitations of claim 27." However, Adams' relying unit receives the pre-qualification privilege data from the centralized privilege data selector and then *compares the test criteria data with the pre-qualification privilege data* as a pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential. Adams clearly teaches that the relying unit performs this comparison on its own. Thus, the relying unit only receives the pre-qualification privilege data from the privilege data selector. Adams does not use the privilege data selector to perform the pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential.

Thus, for at least the reasons above, the rejection of claim 27 is not supported by the prior art and removal thereof is respectfully requested.

Claim 28:

Regarding claim 28, please refer to the arguments above regarding the § 102(a) rejection of claim 2 as they also apply to claim 28. Thus, for at least the reasons above, the rejection of claim 28 is not supported by the prior art and removal thereof is respectfully requested.

Claims 29 and 31:

Regarding claim 29, the § 102(a) rejection of claim 29 is improper since the Examiner, regarding the rejection of claims 3 and 4, which recite subject matter similar to that of claim 29, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service and where the first message corresponds to a message defined in the data representation language schema. Thus, Adams clearly fails to anticipate claim 29. Thus, for at least the reasons above, the rejection of claim 29 is not supported by the prior art and removal thereof is respectfully requested.

Claim 30:

Regarding claim 30, the § 102(a) rejection of claim 30 is improper since the Examiner, regarding the rejection of claim 5 relies upon Czerwinski to teach wherein each one of said additional messages is defined by the data representation language schema. Thus, Adams clearly fails to anticipate claim 30.

In addition, Adams does not mention anything regarding including an authentication credential with each additional message sent by the client to the service. Adams only states that the subscriber unit transmits the pre-qualification attributes or privilege data to the relying unit "through a suitable communication link" (Adams, column 6, line 67 – column 7, line 2). Adams fails to mention anything regarding the sending of additional message or about an authentication credential included in each of the additional messages.

Thus, for at least the reasons above, the rejection of claim 30 is not supported by the cited art and removal thereof is respectfully requested.

Claim 34:

Regarding claim 34, please refer to the arguments above regarding the § 102(a) rejection of claim 9 as they also apply to claim 34. Thus, for at least the reasons above, the rejection of claim 34 is not supported by the cited art and removal thereof is respectfully requested.

Claim 35:

Regarding claim 35, please refer to the arguments above regarding the § 102(a) rejection of claim 10 as they also apply to claim 35. Thus, for at least the reasons above, the rejection of claim 35 is not supported by the cited art and removal thereof is respectfully requested.

Claim 36:

Regarding claim 36, please refer to the arguments above regarding the § 102(a) rejection of claim 12 as they also apply to claim 36. Thus, for at least the reasons above, the rejection of claim 36 is not supported by the cited art and removal thereof is respectfully requested.

Claim 40:

Regarding claim 40, the rejection of claim 40 is improper because the Examiner has failed to provide a *prima facie* rejection. The Examiner states, "claims 27-31, 33-36, and 38-42 encompass the same scope as claims 1-6, 8-11, 15 and 16" and that therefore, "claims 27-31, 33-36, and 38-42 are rejected based on the same reasons set forth in rejecting claims 1-6, 8-11, 15 and 16." **However, none of claims 1-6, 8-11, 15 and 16 recite the limitation of claim 40.** Claim 40 recites where the client device is configured to couple to a network via a wireless connection. Thus, the Examiner has failed to provide a *prima facie* rejection of claim 40.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses the client device is configured to couple to a network via a wireless connection (Adams: column 7 lines 1-2). The communication link incorporates any well known communication method including wireless connection." Applicants respectfully disagree that Adams discloses the client device is configured to couple to a network via a wireless connection. A generic instance (e.g. "a suitable communications link", Adams) is insufficient to teach a specific instance (e.g., a wireless connection).

Thus, for at least the reasons above, the rejection of claim 40 is not supported by the cited art and removal thereof is respectfully requested.

Claims 43, 47, 49 and 50:

Regarding claim 43, Adams fails to disclose a service device configured to determine client capabilities for a client, where the client capabilities are capabilities of the service device that the client is permitted to use. Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams' centralized privilege data selector. However, the cited passage does not describe determining a client's capabilities. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as may be stored in a certificate repository, to the supplied test criteria data. Adams does not describe his privilege data selector as determining client capabilities. Instead, Adams teaches that the privilege data selector selects among subscriber privilege data "based on the privilege test criteria data." Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

Adams also fails to disclose that the service device is configured to bind the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential. The cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit. Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

Additionally, Adams fails to disclose that the service device is configured to use the authentication service to authenticate the authentication credential received in the

message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses determining client capabilities for a client", "Adams also discloses binding the client capabilities to the authentication credential", and "Adams discloses using the authentication service to authenticate the authentication credential". The Examiner's assertions were responded to by Applicants above in regard to claim 27. The arguments given in response to these assertions in regard to claim 27 also apply to claim 43.

Thus, for at least the reasons above, the rejection of claim 43 is not supported by the prior art and removal thereof is respectfully requested.

Claim 44:

Regarding claim 44, the § 102(a) rejection of claim 44 is improper since the Examiner, regarding the rejection of claim 3, which recites subject matter similar to that of claim 44, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service. Thus, Adams clearly fails to anticipate claim 44. Thus, for at least the reasons above, the rejection of claim 44 is not supported by the cited art and removal thereof is respectfully requested.

Claim 45:

Regarding claim 45, the § 102(a) rejection of claim 45 is improper since the Examiner, regarding the rejection of claim 4, which recites subject matter similar to that of claim 45, admits that Adams fails to disclose where the first message corresponds to a message defined in the data representation language schema. Thus, Adams clearly fails to anticipate claim 45. Thus, for at least the reasons above, the rejection of claim 45 is not supported by the cited art and removal thereof is respectfully requested.

Claims 51, 56 and 57:

Regarding claim 51, contrary to the Examiner's assertion, Adams fails to disclose a client device configured to determine client capabilities for a client device, where the client capabilities are capabilities of the service device that the client is permitted to use. Please refer to the arguments above regarding claim 27 for a detailed discussion regarding Adams failure to disclose a client device configured to determine client capabilities for a client device, where the client capabilities are capabilities of the service device that the client is permitted to use, as they also apply to claim 51.

Adams also fails to disclose that the client device is configured to bind the client capabilities to the authentication credential. Please refer to the arguments above

regarding claim 27 for a detailed discussion regarding Adams failure to disclose a client device configured to bind the client capabilities to the authentication credential, as they also apply to claim 51.

Additionally, Adams fails to disclose that the service device is configured to use the authentication service to authenticate the authentication credential received in the message from the client. Please refer to the arguments above regarding claim 27 for a detailed discussion regarding Adams failure to disclose a service device is configured to use the authentication service to authenticate the authentication credential, as they also apply to claim 51.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses determining client capabilities for a client", "Adams also discloses binding the client capabilities to the authentication credential", and "Adams discloses using the authentication service to authenticate the authentication credential". The Examiner's assertions in regard to claim 51 were responded to by Applicants above in regard to claim 27. The arguments given in response to these assertions in regard to claim 27 also apply to claim 51.

Thus, for at least the reasons above, the rejection of claim 51 is not supported by the prior art and removal thereof is respectfully requested.

Claim 52:

Regarding claim 52, the § 102(a) rejection of claim 52 is improper since the Examiner, regarding the rejection of claim 3, which recites subject matter similar to that recited, in part, by claim 52, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service. Thus, Adams clearly fails to anticipate claim 52. Additionally, please refer to the arguments regarding the § 102(a) rejection of claim 2

above, which also apply to claim 52. Thus, for at least the reasons above, the rejection of claim 52 is not supported by the cited art and removal thereof is respectfully requested.

Claims 53 and 55:

Regarding claim 53, the § 102(a) rejection of claim 53 is improper since the Examiner, regarding the rejection of claims 3 and 4, which recite subject matter similar to that of claim 53, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service and where the first message corresponds to a message defined in the data representation language schema. Thus, Adams clearly fails to anticipate claim 53. Thus, for at least the reasons above, the rejection of claim 53 is not supported by the cited art and removal thereof is respectfully requested.

Claim 58:

Regarding claim 58, Adams fails to disclose a client device configured to obtain a service advertisement for a service, where the service advertisement includes an address for an authentication service. The Examiner cites column 31-67. However, the cited passage makes no mention of a client obtaining a service advertisement for a service that includes an address for an authentication service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. No mention is made in the cited passage regarding a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. According to the Examiner's interpretation, Adams' subscriber would have to obtain a service advertisement for the relying party unit and the service advertisement would have to

include an address for the centralized privilege data selector. However, Adams system does not include any service advertisement for a relying party unit that includes an address for the centralized privilege data selector. The Examiner has clearly misinterpreted the teachings of Adams.

Additionally, Adams does not disclose that the client device is configured to generate a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client device to the service device. The Examiner cites column 6, lines 65-67 where Adams states that any matching attribute certificates are sent as pre-qualification privilege data back to the subscriber unit and that the subscriber unit then transmits the pre-qualification privilege data to the relying unit through a suitable communication link. The cited passage does not mention anything about the subscriber unit, which the Examiner considered a client, generating a message gate that embeds the authentication credential in every message from the client to the service. The mere mention of "a suitable communication link" does not disclose the specific limitation of generating a message gate that embeds an authentication credential in every message. Adams does not describe, either at the cited passage or elsewhere, anything about message gates or embedding an authentication credential in every message from a client to a service. The Examiner is merely relying upon speculation, which is clearly improper.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses that the subscriber requests access to the service through a Website and the subscriber provides the identification of the service and subscriber to the authentication service" and "Adams discloses that the pre-qualification privilege data is sent with access request to relying party through suitable communication link and a communication system employing cryptography based security". The Examiner's assertions regarding claim 58 were responded to by Applicants above in regard to claim 17. The arguments given in response to these assertions in regard to claim 17 also apply to claim 58.

Thus, for at least the reasons above, the rejection of claim 58 is not supported by the cited art and removal thereof is respectfully requested.

Claim 59:

Regarding claim 59, please refer to the arguments above regarding the § 102(a) rejection of claim 18 as they also apply to claim 59. Thus, for at least the reasons above, the rejection of claim 59 is not supported by the cited art and removal thereof is respectfully requested.

Claim 61:

Regarding claim 61, Adams fails to disclose the service using the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams

state that the privilege data selector is used as part of this verification.

Adams further fails to disclose where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. The Examiner cites column 7, lines 3-8. However, the cited passage fails to describe the relying unit responding to a request message from the client *only if the request message is for an authorized capability for the client.* Adams teaches that the relying unit sends a confirmation message "indicating whether the relying party has granted privilege to the subscriber unit" (Adams, column 6, lines 25-30). Thus, the relying unit responds to the message (with a confirmation message) whether or not the request message is for an authorized capability for the client. The relying unit may not grant the subscriber unit privilege, but Adams' clearly teaches that it responds with a confirmation message.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses using the authentication service to authenticate the authentication credential" and "Adams discloses that the relying party responds/grants access to the request only if the pre-qualification privilege data contains proper attribute certificates…the definition of 'responds' interpreted by the examiner is when access is granted." The Examiner's assertions regarding claim 61 were responded to by Applicants above in regard to claim 20. The arguments given in response to this assertion in regard to claim 20 also apply to claim 61.

Thus, for at least the reasons above, the rejection of claim 61 is not supported by the cited art and removal thereof is respectfully requested.

Claims 62 and 66:

Regarding claim 62, contrary to the Examiner's assertion, Adams fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use. Adams also fails to

disclose binding the client capabilities to the authentication credential. Additionally, Adams fails to disclose the service using the authentication service to authenticate the authentication credential received in the message from the client. Please refer to the arguments presented above regarding claim 1, as they also apply to claim 62. Thus, for at least the reasons above, the rejection of claim 62 is not supported by the prior art and removal thereof is respectfully requested.

Claim 63:

Regarding claim 63, please refer to the arguments above regarding the § 102(a) rejections of claims 2 and 28 as they also apply to claim 63. Thus, for at least the reasons above, the rejection of claim 63 is not supported by the cited art and removal thereof is respectfully requested.

Claims 64 and 65:

Regarding claim 64, the § 102(a) rejection of claim 64 is improper since the Examiner, regarding the rejection of claims 3 and 4, which recite subject matter similar to that of claim 64, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service and where the first message corresponds to a message defined in the data representation language schema. Thus, Adams clearly fails to anticipate claim 64. Thus, for at least the reasons above, the rejection of claim 64 is not supported by the cited art and removal thereof is respectfully requested.

Claim 67:

Regarding claim 67, please refer to the arguments above regarding the § 102(a) rejection of claim 12 as they also apply to claim 67. Thus, for at least the reasons above, the rejection of claim 67 is not supported by the cited art and removal thereof is respectfully requested.

Claim 69:

Regarding claim 69, Adams fails to disclose a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. Additionally, Adams does not disclose the client generating a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client to the service. Please refer to the arguments presented above regarding claim 17, as they also apply to claim 69. Thus, for at least the reasons above, the rejection of claim 69 is not supported by the cited art and removal thereof is respectfully requested.

Claim 70:

Regarding claim 70, please refer to the arguments above regarding the § 102(a) rejection of claim 18 as they also apply to claim 70. Thus, for at least the reasons above, the rejection of claim 70 is not supported by the cited art and removal thereof is respectfully requested.

Claim 72:

Regarding claim 72, please refer to the arguments above regarding the § 102(a) rejection of claim 61 as they also apply to claim 72. Thus, for at least the reasons above, the rejection of claim 72 is not supported by the cited art and removal thereof is respectfully requested.

Fifth Ground of Rejection

Claims 27-31, 33-36, 38-45, 47, 49-53, 55-59, 61-67, 60, 70 and 72 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of

Czerwinski. Appellants traverse this rejection for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 27, 33, 38, 39, 41 and 42:

Regarding claim 27, Adams in view of Czerwinski fails to teach or suggest a client device configured to determine client capabilities for the client device, where the client capabilities are capabilities of the first service that the client device is permitted to use. As described above regarding claim 1, Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams' centralized privilege data selector. However, the cited passage does not describe determining a client's capabilities. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as may be stored in a certificate repository, to the supplied test criteria data.

Adams does not describe his privilege data selector as determining client capabilities. Instead, Adams teaches that the privilege data selector selects among subscriber privilege data "based on the privilege test criteria data." Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

Adams in view of Czerwinski also fails to teach or suggest the client device configured to bind the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential. The cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit. Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

Additionally, Adams in view of Czerwinski fails to teach or suggest the service configured to use the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in

claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client device configured to determine client capabilities for the client device, where the client capabilities are capabilities of the first service that the client device is permitted to use; the service configured to use the authentication service to authenticate the authentication credential received in the message from the client; and the service configured to use the authentication service to authenticate the authentication credential received in the message from the client. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 27. Thus, for at least the reasons above, the rejection of claim 27 is not supported by the prior art and removal thereof is respectfully requested.

Claim 28:

Regarding claim 28, Adams in view of Czerwinski fails to teach or suggest a client device configured to: obtain an address for said authentication service from an advertisement for said first service; wherein, in said accessing an authentication service, the client device is further configured to: send a message to said address for said authentication service requesting said authentication credential to use said advertised first service. Please refer to the arguments above regarding the § 102(a)

rejection of claim 2 as they also apply to claim 28. Thus, for at least the reasons above, the rejection of claim 28 is not supported by the cited art and removal thereof is respectfully requested.

Claim 29:

Regarding claim 29, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 3 and 4, as they also apply to claim 29. In addition, the § 102(a) rejection of claim 29 is improper since the Examiner, regarding the rejection of claims 3 and 4, which recite subject matter similar to that of claim 29, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service and where the first message corresponds to a message defined in the data representation language schema. Thus, Adams clearly fails to anticipate claim 29. Thus, for at least the reasons above, the rejection of claim 29 is not supported by the cited art and removal thereof is respectfully requested.

Claims 30 and 31:

Regarding claim 30, Adams in view of Czerwinski fails to teach or suggest wherein said first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 5, as they also apply to claim 30. Thus, for at least the reasons above, the rejection of claim 30 is not supported by the cited art and removal thereof is respectfully requested.

Claim 34:

Regarding claim 34, Adams in view of Czerwinski fails to teach or suggest that determining client capabilities includes the client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. The Examiner cites column 6, lines 31-67. The cited passage describes use of a centralized privilege data selector in Adams' system. Adams teaches that a relying unit communicates privilege test criteria data to the centralized privilege data selector and that a subscriber unit sends privilege verification request data including subscriber identification data and selected relying party identification data to the centralized privilege data selector. The centralized privilege data selector uses the subscriber identification data to obtain the appropriate attribute certificates from an attributes certificate repository and uses the relying party identification data to obtain the correct privilege test data for the identified relying party unit. However, the cited passage does not mention a client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. Adams' centralized privilege data selector sends attribute certificates that match the privilege test data to the subscriber unit. Nowhere does Adams mention a client obtaining a capability token indicating which capabilities of the service the client is permitted to access. Adams attribute certificates include such certificates as Kerberos tickets, DCE PAC, etc. that do not indicate which capabilities of a service the client is permitted to access.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest that determining client capabilities includes the client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 34. Thus, for at least the reasons above, the rejection of claim 34 is not supported by the cited art and removal thereof is respectfully requested.

Claim 35:

Regarding claim 35, Adams in view of Czerwinski fails to teach or suggest an authentication service and an access policy service that are combined as a single service and where the capability token is included within the authentication credential. The Examiner cites column 6, lines 31-67. However, the cited passage fails to mention anything about an authentication service and an access policy service combined as a single service. The cited passage also fails to mention a capability token included within an authentication credential. The cited passage describes centralized privilege data selector that receives information from both a relying unit and subscriber unit and that returns matching attribute certificates to the subscriber unit. Nowhere does Adams describe either a combined authentication service and access policy service or a capability token included within an authentication credential.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest an authentication service and an access policy service that are combined as a single service and where the capability token is included within the authentication credential. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 35. Thus, for at least the reasons above, the rejection of claim 35 is not supported by the cited art and removal thereof is respectfully requested.

Claim 36:

Regarding claim 36, Adams in view of Czerwinski fails to teach or suggest the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential in each message to the first service. The Examiner cites column 6, line 67 – column 7, line 8 of Adams. However, the cited passage makes no mention whatsoever regarding a client generating a message gate or about the message gate including an authentication credential in each message to the service. The cited passage merely states that Adams' subscriber unit

sends pre-qualification attributes or privilege data to the relying unit "through a suitable communication link". However, merely stating that the pre-qualification attributes are sent through a suitable communication link does not disclose the specific limitations of generating a message gate or about a message gate including an authentication credential in each message to the service. Nowhere does Adams mention anything regarding either message gates or about including an authentication credential in each message to the first service.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential **in each message** to the first service. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 36. Thus, for at least the reasons above, the rejection of claim 36 is not supported by the cited art and removal thereof is respectfully requested.

Claim 40:

Regarding claim 40, the rejection of claim 40 is improper because the Examiner has failed to provide a *prima facie* rejection. The Examiner states, "claims 27-31, 33-36, and 38-42 encompass the same scope as claims 1-6, 8-11, 15 and 16" and that therefore, "claims 27-31, 33-36, and 38-42 are rejected based on the same reasons set forth in rejecting claims 1-6, 8-11, 15 and 16." However, none of claims 1-6, 8-11, 15 and 16 recite the limitation of claim 40. Claim 40 recites where the client device is configured to couple to a network via a wireless connection. Thus, the Examiner has failed to provide a *prima facie* rejection of claim 40.

Furthermore, Adams and Czerwinski, whether considered singly or in combination, fails to teach or suggest a client device configured to couple to a network via a wireless connection.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses the client device is configured to couple to a network via a wireless connection (Adams: column 7 lines 1-2). The communication link incorporates any well known communication method including wireless connection." Applicants respectfully disagree that Adams discloses the client device is configured to couple to a network via a wireless connection. A generic instance (e.g. "a suitable communications link", Adams) is insufficient to teach a specific instance (e.g., a wireless connection).

Thus, for at least the reasons above, the rejection of claim 40 is not supported by the cited art and removal thereof is respectfully requested.

Claims 43, 47, 49 and 50:

Regarding claim 43, Adams in view of Czerwinski fails to disclose a service device configured to determine client capabilities for a client, where the client capabilities are capabilities of the service device that the client is permitted to use. Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams'

centralized privilege data selector. However, the cited passage does not describe determining a client's capabilities. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as may be stored in a certificate repository, to the supplied test criteria data. Adams does not describe his privilege data selector as determining client capabilities. Instead, Adams teaches that the privilege data selector selects among subscriber privilege data "based on the privilege test criteria data." Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

Adams also fails to disclose that the service device is configured to bind the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential. The cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit. Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

Additionally, Adams fails to disclose that the service device is configured to use the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches

that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses determining client capabilities for a client", "Adams also discloses binding the client capabilities to the authentication credential", and "Adams discloses using the authentication service to authenticate the authentication credential". The Examiner's assertions were responded to by Applicants above in regard to claim 27. The arguments given in response to these assertions in regard to claim 27 also apply to claim 43.

Thus, for at least the reasons above, the rejection of claim 43 is not supported by the prior art and removal thereof is respectfully requested.

Claim 44:

Regarding claim 44, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Please refer to the arguments presented above regarding claim 3, as they also apply to claim 44. Thus, for at least the reasons above, the rejection of claim 44 is not supported by the cited art and removal thereof is respectfully requested.

Claim 45:

Regarding claim 45, Adams in view of Czerwinski fails to teach or suggest wherein said first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 5, as they also apply to claim 45. Thus, for at least the reasons above, the rejection of claim 45 is not supported by the cited art and removal thereof is respectfully requested.

Claims 51, 56 and 57:

Regarding claim 51, contrary to the Examiner's assertion, Adams in view of Czerwinski fails to teach or suggest a client device configured to determine client capabilities for a client device, where the client capabilities are capabilities of the service device that the client is permitted to use. Please refer to the arguments above regarding claim 27 for a detailed discussion regarding Adams failure to disclose a client device configured to determine client capabilities for a client device, where the client capabilities are capabilities of the service device that the client is permitted to use, as they also apply to claim 51.

Adams in view of Czerwinski also fails to teach or suggest that the client device is configured to bind the client capabilities to the authentication credential. Please refer to

the arguments above regarding claim 27 for a detailed discussion regarding Adams failure to disclose a client device configured to bind the client capabilities to the authentication credential, as they also apply to claim 51.

Additionally, Adams in view of Czerwinski fails to teach or suggest that the service device is configured to use the authentication service to authenticate the authentication credential received in the message from the client. Please refer to the arguments above regarding claim 27 for a detailed discussion regarding Adams failure to disclose a service device is configured to use the authentication service to authenticate the authentication credential, as they also apply to claim 51.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses determining client capabilities for a client", "Adams also discloses binding the client capabilities to the authentication credential", and "Adams discloses using the authentication service to authenticate the authentication credential". The Examiner's assertions in regard to claim 51 were responded to by Applicants above in regard to claim 27. The arguments given in response to these assertions in regard to claim 27 also apply to claim 51.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client device configured to determine client capabilities for a client device, where the client capabilities are capabilities of the service device that the client is permitted to use; that the client device is configured to bind the client capabilities to the authentication credential and that the service device is configured to use the authentication service to authenticate the authentication credential received in the message from the client. Thus, Czerwinski fails to over the above noted deficiencies of Adams regarding the limitations of claim 51. No combination of Adams and Czerwinski teach or suggests the limitations of claim 51. Thus, for at least the reasons above, the rejection of claim 51 is not supported by the prior art and removal thereof is respectfully requested.

Claim 52:

Regarding claim 52, Adams in view of Czerwinski fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service. The Examiner cites FIG. 5 and column 6, lines 31-40 of Adams. However, the cited portions make no mention of a client obtaining an address for the authentication service from an advertisement for the service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. Nowhere does Adams describe a client obtaining an address for the authentication service from an advertisement for the service.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service. Thus, Czerwinski fails to over the above noted deficiencies of Adams.

Adams in view of Czerwinski further fails to teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach or suggest an advertisement for the first service that includes a data representation language schema defining a message interface for accessing the first service and relies upon Czerwinski. However, Czerwinski does not teach that the advertisement for the first service includes a data representation language schema

defining a message interface for accessing the first service. In contrast, Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.

Furthermore, no combination of Adams and Czerwinski teaches or suggests a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service and that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service.

In addition, the § 102(a) rejection of claim 52 is improper since the Examiner, regarding the rejection of claim 3, which recites subject matter similar to that recited, in part, by claim 52, admits that Adams fails to disclose an advertisement for the service that includes a data representation language schema defining a message interface for accessing the first service. Thus, Adams clearly fails to anticipate claim 52.

Thus, for at least the reasons above, the rejection of claim 52 is not supported by the cited art and removal thereof is respectfully requested.

Claims 53 and 55:

Regarding claim 53, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation

language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claims 3 and 4, as they also apply to claim 53. Thus, for at least the reasons above, the rejection of claim 53 is not supported by the cited art and removal thereof is respectfully requested.

Claim 58:

Regarding claim 58, Adams in view of Czerwinski fails to teach or suggest a client device configured to obtain a service advertisement for a service, where the service advertisement includes an address for an authentication service. The Examiner cites column 31-67. However, the cited passage makes no mention of a client obtaining a service advertisement for a service that includes an address for an authentication service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. No mention is made in the cited passage regarding a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. According to the Examiner's interpretation, Adams' subscriber would have to obtain a service advertisement for the relying party unit and the service advertisement would have to include an address for the centralized privilege data selector. However, Adams system does not include any service advertisement for a relying party unit that includes an address for the centralized privilege data selector. The Examiner has clearly misinterpreted the teachings of Adams.

Additionally, Adams in view of Czerwinski does not teach or suggest that the client device is configured to generate a message gate for accessing the service, where the

message gate embeds the authentication credential in *every* message from the client device to the service device. The Examiner cites column 6, lines 65-67 where Adams states that any matching attribute certificates are sent as pre-qualification privilege data back to the subscriber unit and that the subscriber unit then transmits the pre-qualification privilege data to the relying unit through a suitable communication link. The cited passage does not mention anything about the subscriber unit, which the Examiner considered a client, generating a message gate that embeds the authentication credential in every message from the client to the service. The mere mention of "a suitable communication link" does not disclose the specific limitation of generating a message gate that embeds an authentication credential in every message. Adams does not describe, either at the cited passage or elsewhere, anything about message gates or embedding an authentication credential in every message from a client to a service. The Examiner is merely relying upon speculation, which is clearly improper.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams discloses that the subscriber requests access to the service through a Website and the subscriber provides the identification of the service and subscriber to the authentication service" and "Adams discloses that the pre-qualification privilege data is sent with access request to relying party through suitable communication link and a communication system employing cryptography based security". The Examiner's assertions regarding claim 58 were responded to by Applicants above in regard to claim 17. The arguments given in response to these assertions in regard to claim 17 also apply to claim 58.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client device configured to obtain a service advertisement for a service, where the service advertisement includes an address for an authentication service; and that that the client device is configured to generate a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client device to the service device. Thus, Czerwinski fails to over the above noted deficiencies of Adams regarding the limitations of claim 58. No combination of Adams and

Czerwinski teach or suggests the limitations of claim 58. Thus, for at least the reasons above, the rejection of claim 58 is not supported by the prior art and removal thereof is respectfully requested.

Claim 59:

Regarding claim 59, Adams in view of Czerwinski fails to teach or suggest wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said service device; and wherein said message gate is further configured to verify that every message sent from said client device to said service device complies with said data representation language schema. Please refer to the arguments presented above regarding claim 18, as they also apply to claim 59. Thus, for at least the reasons above, the rejection of claim 59 is not supported by the cited art and removal thereof is respectfully requested.

Claim 61:

Regarding claim 61, Adams in view of Czerwinski fails to teach or suggest the service using the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the

relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

Adams in view of Czerwinski further fails to teach or suggest where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. The Examiner cites column 7, lines 3-8. However, the cited passage fails to describe the relying unit responding to a request message from the client *only if the request message is for an authorized capability for the client.* Adams teaches that the relying unit sends a confirmation message "indicating whether the relying party has granted privilege to the subscriber unit" (Adams, column 6, lines 25-30). Thus, the relying unit responds to the message (with a confirmation message) whether or not the request message is for an authorized capability for the client. The relying unit may not grant the subscriber unit privilege, but Adams' clearly teaches that it responds with a confirmation message.

In the Examiner's Answer dated October 4, 2006, the Examiner asserts "Adams clearly discloses using the authentication service to authenticate the authentication credential" and "Adams discloses that the relying party responds/grants access to the request only if the pre-qualification privilege data contains proper attribute certificates…the definition of 'responds' interpreted by the examiner is when access is granted." The Examiner's assertions regarding claim 61 were responded to by Applicants above in regard to claim 20. The arguments given in response to this assertion in regard to claim 20 also apply to claim 61.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest the service using the authentication service to authenticate the authentication credential

received in the message from the client and where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. Thus, Czerwinski fails to over the above noted deficiencies of Adams regarding the limitations of claim 61. No combination of Adams and Czerwinski teach or suggests the limitations of claim 61. Thus, for at least the reasons above, the rejection of claim 61 is not supported by the cited art and removal thereof is respectfully requested.

Claims 62 and 66:

Regarding claim 62, contrary to the Examiner's assertion, Adams in view of Czerwinski fails to teach or suggest determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use. Adams in view of Czerwinski also fails to teach or suggest binding the client capabilities to the authentication credential. Additionally, Adams in view of Czerwinski fails to teach or suggest the service using the authentication service to authenticate the authentication credential received in the message from the client. Please refer to the arguments presented above regarding claim 1, as they also apply to claim 62. Thus, for at least the reasons above, the rejection of claim 62 is not supported by the prior art and removal thereof is respectfully requested.

Claim 63:

Regarding claim 63, Adams in view of Czerwinski fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service. The Examiner cites FIG. 5 and column 6, lines 31-40 of Adams. However, the cited portions make no mention of a client obtaining an address for the authentication service from an advertisement for the service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a

subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. Nowhere does Adams describe a client obtaining an address for the authentication service from an advertisement for the service.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 63. Thus, for at least the reasons above, the rejection of claim 63 is not supported by the cited art and removal thereof is respectfully requested.

Claims 64 and 65:

Regarding claim 64, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claims 3 and 4, as they also apply to claim 64. Thus, for at least the reasons above, the rejection of claim 64 is not supported by the cited art and removal thereof is respectfully requested.

Claim 67:

Regarding claim 67, Adams in view of Czerwinski fails to teach or suggest the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential in each message to the

first service. The Examiner cites column 6, line 67 – column 7, line 8 of Adams. However, the cited passage makes no mention whatsoever regarding a client generating a message gate or about the message gate including an authentication credential in each message to the service. The cited passage merely states that Adams' subscriber unit sends pre-qualification attributes or privilege data to the relying unit "through a suitable communication link". However, merely stating that the pre-qualification attributes are sent through a suitable communication link does not disclose the specific limitations of generating a message gate or about a message gate including an authentication credential in each message to the service. Nowhere does Adams mention anything regarding either message gates or about including an authentication credential in each message to the first service.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential **in each message** to the first service. Thus, the combination of Adams and Czerwinski also fails to teach or suggest the limitations of claim 67. Thus, for at least the reasons above, the rejection of claim 67 is not supported by the cited art and removal thereof is respectfully requested.

Claim 69:

Regarding claim 69, Adams in view of Czerwinski fails to teach or suggest a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. Additionally, Adams does not disclose the client generating a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client to the service. Please refer to the arguments presented above regarding claim 17, as they also apply to claim 69. Thus, for at least the reasons above, the rejection of claim 69 is not supported by the cited art and removal thereof is respectfully requested.

Claim 70:

Regarding claim 70, Adams in view of Czerwinski fails to teach or suggest wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said service device; and wherein said message gate is further configured to verify that every message sent from said client device to said service device complies with said data representation language schema. Please refer to the arguments presented above regarding claim 18, as they also apply to claim 70. Thus, for at least the reasons above, the rejection of claim 70 is not supported by the cited art and removal thereof is respectfully requested.

Claim 72:

Regarding claim 72, Adams in view of Czerwinski fails to teach or suggest the service using the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1. Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the

attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

Adams in view of Czerwinski further fails to teach or suggest where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. The Examiner cites column 7, lines 3-8. However, the cited passage fails to describe the relying unit responding to a request message from the client *only if the request message is for an authorized capability for the client.* Adams teaches that the relying unit sends a confirmation message "indicating whether the relying party has granted privilege to the subscriber unit" (Adams, column 6, lines 25-30). Thus, the relying unit responds to the message (with a confirmation message) whether or not the request message is for an authorized capability for the client. The relying unit may not grant the subscriber unit privilege, but Adams' clearly teaches that it responds with a confirmation message.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest the service using the authentication service to authenticate the authentication credential received in the message from the client and where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. Thus, Czerwinski fails to over the above noted deficiencies of Adams regarding the limitations of claim 72. No combination of Adams and Czerwinski teach or suggests the limitations of claim 72. Thus, for at least the reasons above, the rejection of claim 72 is not supported by the cited art and removal thereof is respectfully requested.

CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-6, 8-31, 33-47 and 49-72 was erroneous, and reversal of his decision is respectfully requested.

No fee should be due for this appeal brief since the appeal brief fee was already paid for a previous appeal in this application that did not receive a decision on the merits and from which prosecution was reopened. ***See*** **MPEP 1207.04.** However, the Commissioner is authorized to any fee that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-64800/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Appellants

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
(512) 853-8850

Date: July 10, 2007

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A method for communicating in a distributed computing environment, comprising:

a client accessing an authentication service to obtain an authentication credential to use a first service;

determining client capabilities for said client, wherein said client capabilities are capabilities of said first service that said client is permitted to use;

binding said client capabilities to said authentication credential;

said client sending a first message to said first service, wherein said first message includes said authentication credential;

said first service using said authentication service to authenticate said authentication credential received in said first message; and

said first service responding to said first message if said authentication credential in said first message is determined to be authentic as from said client.

2. The method as recited in claim 1, further comprising said client obtaining an address for said authentication service from an advertisement for said first service, wherein said accessing an authentication service comprises said client sending a message to said address for said authentication service requesting said authentication credential to use said advertised first service.

3. The method as recited in claim 2, wherein said advertisement for said first service includes a data representation language schema defining a message interface for accessing said first service.

4. The method as recited in claim 3, wherein said first message corresponds to a message defined in said data representation language schema.

5. The method as recited in claim 4, further comprising said client sending additional messages to said first service to use said first service, wherein said authentication credential is included with each one of said additional messages, and wherein each one of said additional messages is defined by said data representation language schema.

6. The method as recited in claim 5, wherein said data representation language schema is an eXtensible Markup Language (XML) schema.

8. The method as recited in claim 1, further comprising:

said client sending a request message to said first service to access a capability of said first service, wherein said request message includes said authentication credential;

said first service determining that the capability requested in said request message is within said client capabilities; and

said first service fulfilling said request message only if the capability requested in said request message is within said client capabilities.

9. The method as recited in claim 1, wherein said determining client capabilities comprises said client accessing an access policy service to obtain a capability token indicating which capabilities of said first service said client is permitted to access.

10. The method as recited in claim 9, wherein said authentication service and said access policy service are combined as a single service and wherein said capability token is included within said authentication credential.

11. The method as recited in claim 1, wherein said determining client capabilities is performed by said first service.

12. The method as recited in claim 1, further comprising said client generating a message gate for accessing said first service, wherein said message gate sends request messages from said client to said first service to access said first service, and wherein said message gate includes said authentication credential in each message to said first service.

13. The method as recited in claim 12, further comprising said client obtaining a service advertisement for said first service before accessing said first service, wherein said service advertisement comprises an address for said authentication service and an address for said first service.

14. The method as recited in claim 13, wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said first service, wherein said message gate verifies that each message sent from said client to said first service complies with said data representation language schema.

15. The method as recited in claim 1, wherein said authentication service is a separately addressable service from said first service.

16. The method as recited in claim 1, wherein said client accessing an authentication service to obtain an authentication credential to use a first service

comprises said authentication service returning said authentication credential to said client only if said client is authorized to access said first service.

17. A method for communication in a distributed computing environment, comprising:

a client obtaining a service advertisement for a first service, wherein said service advertisement includes an address for an authentication service;

said client sending a request message to said authentication service to obtain an authentication credential to use said first service;

said client generating a message gate for accessing said first service, wherein said message gate embeds said authentication credential in every message from said client to said first service; and

said client accessing said first service through said message gate.

18. The method as recited in claim 17, wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said first service, the method further comprising said message gate verifying that every message sent from said client to said first service complies with said data representation language schema.

19. The method as recited in claim 18, wherein said data representation language schema is an eXtensible Markup Language (XML) schema and said messages from said client to said first service are XML messages.

20. The method as recited in claim 17, further comprising said first service using said authentication service to determine if said authentication credential received in a first message from said client is authentic.

21. The method as recited in claim 20, further comprising, after authenticating said authentication credential received in said first message from said client, said first service determining which capabilities of said first service said client is authorized to use, wherein said first service responds to a request message from said client only if said request message is for an authorized capability for said client.

22. The method as recited in claim 21, further comprising said first service binding a determination of which capabilities of said first service said client is authorized to use to said authentication credential so that said first service does not need to repeat said determining which capabilities of said first service said client is authorized to use.

23. The method as recited in claim 20, further comprising said first service noting whether or not said authentication credential is authentic so that said first service does not need to repeat said using said authentication service to determine if said authentication credential received in a first message from said client is authentic.

24. The method as recited in claim 17, wherein said service advertisement for said first service further includes an address for accessing said first service, wherein said authentication service and said first service are separate services within the distributed computing environment.

25. The method as recited in claim 17, wherein said service advertisement further includes a service identifier token for said first service, wherein said client sending a request message to said authentication service to obtain an authentication credential comprises sending said service identifier token and a client identifier token to said authentication service.

26. The method as recited in claim 25, wherein said authentication service generates said authentication credential from said client identifier token and said service identifier token.

27. A client device configured to:

access an authentication service to obtain an authentication credential to use a first service;

determine client capabilities for said client device, wherein said client capabilities are capabilities of said first service that said client device is permitted to use; and

bind said client capabilities to said authentication credential;

send a first message to said first service, wherein said first message includes said authentication credential, wherein said first service is configured to use said authentication service to authenticate said authentication credential received in said first message; and

receive a response to said first message from said first service if said authentication credential in said first message is determined to be authentic as from said client device.

28. The client device as recited in claim 27, further configured to:

obtain an address for said authentication service from an advertisement for said first service;

wherein, in said accessing an authentication service, the client device is further configured to:

send a message to said address for said authentication service requesting said authentication credential to use said advertised first service.

29. The client device as recited in claim 28, wherein said advertisement for said first service includes a data representation language schema defining a message interface for accessing said first service, and wherein said first message corresponds to a message defined in said data representation language schema.

30. The client device as recited in claim 29, further configured to send additional messages to said first service to use said first service, wherein said authentication credential is included with each one of said additional messages, and wherein each one of said additional messages is defined by said data representation language schema.

31. The client device as recited in claim 29, wherein said data representation language schema is an eXtensible Markup Language (XML) schema.

33. The client device as recited in claim 27, further configured to:

send a request message to said first service to access a capability of said first service, wherein said request message includes said authentication credential;

wherein said first service is configured to fulfill said request message only if said first service determines that the capability requested in said request message is within said client capabilities.

34. The client device as recited in claim 27, wherein, in said determining client capabilities, the client device is further configured to access an access policy service to obtain a capability token indicating which capabilities of said first service said client is permitted to access.

35. The client device as recited in claim 34, wherein said authentication service and said access policy service are combined as a single service, and wherein said capability token is included within said authentication credential.

36. The client device as recited in claim 27, further configured to generate a message gate for accessing said first service, wherein said message gate sends request messages from said client to said first service to access said first service, and wherein said message gate includes said authentication credential in each message to said first service.

37. The client device as recited in claim 36, further configured to:

obtain a service advertisement for said first service before accessing said first service, wherein said service advertisement comprises a data representation language schema defining a message interface for accessing said first service;

wherein said message gate is configured to verify that each message sent from said client device to said first service complies with said data representation language schema.

38. The client device as recited in claim 27, wherein, in said accessing an authentication service to obtain an authentication credential to use a first service, the client device is further configured to receive from said authentication service said authentication credential only if said client device is authorized to access said first service.

39. The client device as recited in claim 27, wherein said authentication service and said first service are configured to execute within a service device, and wherein said client device is further configured to couple to said service device via a network.

40. The client device as recited in claim 27, wherein said client device is further configured to couple to a network via a wireless connection.

41. The client device as recited in claim 27,

wherein said authentication service is configured to execute within an authentication server;

wherein said first service is configured to execute within a service device; and

wherein said client device, said service device, and said authentication server are separate devices comprised in a distributed computing environment.

42. The client device as recited in claim 27, wherein said first service is configured to execute within said client device.

43. A service device configured to:

receive from a client a first message including an authentication credential, wherein said client accesses an authentication service to obtain said authentication credential to use said service device;

use said authentication service to authenticate said authentication credential received in said first message;

determine client capabilities for said client, wherein said client capabilities are capabilities of said service device that said client is permitted to use;

bind said client capabilities to said authentication credential; and

respond to said first message if said authentication credential in said first message is determined to be authentic as from said client.

44. The service device as recited in claim 43, further configured to provide to said client an advertisement for said service device, wherein said advertisement includes a data representation language schema defining a message interface for accessing said service device.

45. The service device as recited in claim 44, wherein said first message corresponds to a message defined in said data representation language schema.

46. The service device as recited in claim 45, further configured to receive additional messages from said client to use said service device, wherein said authentication credential is included with each one of said additional messages, and wherein each one of said additional messages is defined by said data representation language schema.

47. The service device as recited in claim 44, wherein said data representation language schema is an eXtensible Markup Language (XML) schema.

49. The service device as recited in claim 43, further configured to:

receive from said client a request message to access a capability of said service device, wherein said request message includes said authentication credential;

determine that the capability requested in said request message is within said client capabilities; and

fulfill said request message only if the capability requested in said request message is within said client capabilities.

50. The service device as recited in claim 43, wherein said client is configured to execute within a client device, and wherein said service device and said client device are separate devices comprised in a distributed computing environment.

51. A distributed computing system, comprising:

a client device; and

a service device;

wherein said client device is configured to:

access an authentication service to obtain an authentication credential to use said service device;

determine client capabilities for said client device, wherein said client capabilities are capabilities of said service device that said client device is permitted to use;

bind said client capabilities to said authentication credential;

send a first message to said service device, wherein said first message includes said authentication credential; and

wherein said service device is configured to:

use said authentication service to authenticate said authentication credential received in said first message; and

respond to said first message if said authentication credential in said first message is determined to be authentic as from said client.

52. The system as recited in claim 51,

wherein the service device is further configured to provide to said client device an advertisement for said service device, wherein said advertisement includes a data representation language schema defining a message interface for accessing said service device;

wherein the client device is further configured to obtain an address for said authentication service from said advertisement for said service device; and

wherein, in said accessing an authentication service, the client device is further configured to send a message to said address for said authentication service requesting said authentication credential to use said advertised service device.

53. The system as recited in claim 52, wherein said advertisement for said service device includes a data representation language schema defining a message interface for accessing said service device, wherein said first message corresponds to a message defined in said data representation language schema.

54. The system as recited in claim 53, wherein the client device is further configured to send additional messages to said service device to use said service device, wherein said authentication credential is included with each one of said additional messages, and wherein each one of said additional messages is defined by said data representation language schema.

55. The system as recited in claim 53, wherein said data representation language schema is an eXtensible Markup Language (XML) schema.

56. The system as recited in claim 51, wherein said authentication service is configured to execute within said service device.

57. The system as recited in claim 51,

wherein said authentication service is configured to execute within an authentication server; and

wherein said client device, said service device, and said authentication server are separate devices comprised in a distributed computing environment.

58. A distributed computing system, comprising:

a client device;

a service device;

wherein said client device is configured to:

obtain a service advertisement for said service device, wherein said service advertisement includes an address for an authentication service;

send a request message to said authentication service to obtain an authentication credential to use said service device;

generate a message gate for accessing said service device, wherein said message gate is configured to embed said authentication credential in every message from said client device to said service device; and

access said service device through said message gate;

59. The system as recited in claim 58,

wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said service device; and

wherein said message gate is further configured to verify that every message sent from said client device to said service device complies with said data representation language schema.

60. The system as recited in claim 59, wherein said data representation language schema is an eXtensible Markup Language (XML) schema and said messages from said client device to said service device are XML messages.

61. The system as recited in claim 58, wherein said service device is configured to:

use said authentication service to determine if said authentication credential received in a first message from said client device is authentic;

determine which capabilities of said service device said client device is authorized to use; and

respond to said first message from said client device only if said first message is for an authorized capability for said client device.

62. A computer-readable, storage medium comprising program instructions, wherein the program instructions are computer-executable to implement:

a client accessing an authentication service to obtain an authentication credential to use a first service;

determining client capabilities for said client, wherein said client capabilities are capabilities of said first service that said client is permitted to use;

binding said client capabilities to said authentication credential;

said client sending a first message to said first service, wherein said first message includes said authentication credential;

said first service using said authentication service to authenticate said authentication credential received in said first message; and

said first service responding to said first message if said authentication credential in said first message is determined to be authentic as from said client.

63. The computer-readable, storage medium as recited in claim 62, wherein the program instructions are further computer-executable to implement:

said client obtaining an address for said authentication service from an advertisement for said first service;

wherein, in said accessing an authentication service, the program instructions are further computer-executable to implement:

said client sending a message to said address for said authentication service requesting said authentication credential to use said advertised first service.

64. The computer-readable, storage medium as recited in claim 63, wherein said advertisement for said first service includes a data representation language schema defining a message interface for accessing said first service, wherein said first message corresponds to a message defined in said data representation language schema.

65. The computer-readable, storage medium as recited in claim 64, wherein said data representation language schema is an eXtensible Markup Language (XML) schema.

66. The computer-readable, storage medium as recited in claim 62, wherein the program instructions are further computer-executable to implement:

said client sending a request message to said first service to access a capability of said first service, wherein said request message includes said authentication credential;

said first service determining that the capability requested in said request message is within said client capabilities; and

said first service fulfilling said request message only if the capability requested in said request message is within said client capabilities.

67. The computer-readable, storage medium as recited in claim 62, wherein the program instructions are further computer-executable to implement:

said client generating a message gate for accessing said first service;

said message gate sending request messages from said client to said first service to access said first service, wherein said message gate includes said authentication credential in each message to said first service.

68. The computer-readable, storage medium as recited in claim 67, wherein the program instructions are further computer-executable to implement:

said message gate verifying that each message sent from said client to said first service complies with a data representation language schema, wherein said data representation language schema defines a message interface for accessing said first service

69. A computer-readable, storage medium comprising program instructions, wherein the program instructions are computer-executable to implement:

a client obtaining a service advertisement for a first service, wherein said service advertisement includes an address for an authentication service;

said client sending a request message to said authentication service to obtain an authentication credential to use said first service;

said client generating a message gate for accessing said first service, wherein said message gate embeds said authentication credential in every message from said client to said first service; and

said client accessing said first service through said message gate.

70. The computer-readable, storage medium as recited in claim 69, wherein said service advertisement further comprises a data representation language schema defining a message interface for accessing said first service, and wherein the program instructions are further computer-executable to implement:

said message gate verifying that every message sent from said client to said first service complies with said data representation language schema.

71. The computer-readable, storage medium as recited in claim 70, wherein said data representation language schema is an eXtensible Markup Language (XML) schema and said messages from said client to said first service are XML messages.

72. The computer-readable, storage medium as recited in claim 69, wherein the program instructions are further computer-executable to implement:

said first service using said authentication service to determine if said authentication credential received in a first message from said client is authentic;

said first service determining which capabilities of said first service said client is authorized to use; and

said first service responding to said first message from said client only if said first message is for an authorized capability for said client.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131 or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.